



---

## KVM Switch CAT-32 IP with KVM over IP Module

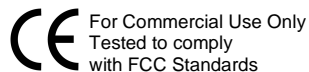
User Manual

*English*

---

KVM Switch CAT-32 IP: LINDY No. 39632  
KVM over IP Module: LINDY No. 39636

**[www.lindy.com](http://www.lindy.com)**



### The modular LINDY KVM Switch CAT-32 IP

The KVM Switch CAT-32 IP provides 32 Cat.5/6 KVM server ports supporting both USB or PS/2 keyboard and mouse connections via dedicated USB or PS/2 Cat.5 Computer Modules.

This KVM switch incorporates a modular concept design which allows for dual console access. The local console port allows direct access whilst a second console option permits remote access via a remote KVM over IP module installed in a slot located in the back of the KVM Switch. This option allows system administrators to access and administer their servers and KVM switches from a remote office computer via a web browser. The required optional IP access module can be simply installed into the back of the KVM Switch at any time.

### About this manual

This manual is divided into five sections.

- The first section is an introduction to the KVM Switch CAT-32
- The second section deals with installing and connecting the switch
- The third section describes the basic operation of the KVM switch via its OSD (On Screen Menu)
- Section 4 – left empty for future use
- The fifth section describes operation and access via remote IP

### Technological progress

The KVM Switch and especially the KVM over IP Module and its software are subject to technological progress. The products are continuously upgraded accordingly. Therefore minor changes compared to the descriptions in this manual may be found.

**Contents**

**Section 1.....3**  
1.1 Introduction.....4  
1.2 CAT-32 with IP access module.....5  
1.3 KVM compatibility with other series KVM switches.....5  
1.4 Product Features .....6  
1.5 Package Contents .....7  
1.5 Optional Cables and Accessories .....7

**Section 2.....8**  
2.1 Hardware Installation Guide .....9

**Section 3.....10**  
3.1 KVM Switch Operation.....11  
3.2 Keyboard Hotkey Selection and OSD Commands.....12  
3.3 On Screen Display Menu (OSD) .....13  
3.4 Troubleshooting.....14

**Section 4.....15**  
Intentionally left empty

**Section 5.....15**  
5.0.1 KVM over IP Access Features .....16  
5.0.2 KVM over IP Module Installation.....16  
5.1 Configuration .....17  
5.2 CAT-32 IP Setup Tool.....18  
5.3 Keyboard, Mouse and Video Configuration .....20  
5.4 Usage .....22  
5.5 Logging In .....23  
5.6 Navigation .....24  
5.7 Menu Options .....31  
5.7.1 Remote Control.....31  
5.7.2 Virtual Media.....34  
5.7.3 User Management .....42  
5.7.4 KVM Settings .....44  
5.7.5 Device Settings.....49  
5.7.6 Maintenance .....62

**Troubleshooting .....66**

**Key Codes .....70**

**Section 1**

**Introducing the  
KVM Switch  
CAT-32 IP**

## 1.1. Introduction

Thank you for purchasing this LINDY KVM Switch. Please read this manual carefully to fully understand the functions and features that the switch offers.

Using the LINDY KVM Switch CAT-32 IP a system administrator can access and control several computers from one compact and high density KVM control center with 32 server ports occupying only 1U height within a 19" rack.

In addition the KVM Switch CAT-32 allows you to install an optional KVM over IP Remote Access Module into a slot located in the back of the KVM switch. With this module installed the administrator can access any of the computers connected to the KVM Switch from any remote computer on a local LAN or via the Internet using a web browser.

The LINDY KVM Switch CAT-32 allows direct access to up to 32 computers using a single KVM (Keyboard, Video, and Mouse) either from a local or remote console. To administrate a larger number of computers multiple switches can be used. They can be either equipped with a KVM over IP module each or they can easily be daisy chained with an IP module located in the master KVM switch only.

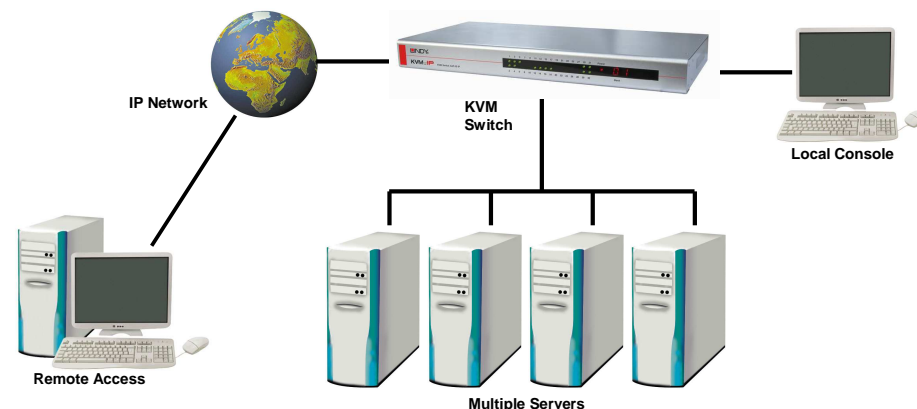
A dedicated daisy chain port allows a total number of 8 KVM Switches to be connected (daisy chained) together to control up to 256 computers. Using this daisy chain port method ensures that none of the computer ports are lost due to cascading. Using IP modules in each KVM Switch allows users to access even more than 256 computers and provides individual simultaneous access to every KVM switch with an IP module and by several users.

The CAT-32 KVM Switch supports two methods of switching between the connected computers: by using keyboard hotkeys or via an OSD (On Screen Display).

The KVM Switch CAT-32 IP has a single user password protection with auto logout security. The security features for the KVM over IP user are based on SSL and additionally KVM encrypted connections with a further level of password login.

## 1.2. CAT-32 with IP access module

KVM over IP technology allows a simple web browser interface to be used to access the switch and the connected computers via a local area network (LAN) or, when connected to a wide area network (WAN), allows access to the switch and the connected computers from almost anywhere in the world.



**Remote & local control of multiple computers**

The CAT-32 with IP module provides a non-intrusive solution for remote access and control because the software runs on its embedded processors only, so there's no interference with computer operation, or impact on network performance. The IP module also features remote mass storage support; a USB connection from the switch to a connected computer allows virtual storage to be set up on the computer as a virtual drive accessed from the client.

Doing so any files, folders or local drives at the remote user can be configured as a local drive at the remote computer allowing for driver installation and updates etc.

## 1.3. KVM compatibility with other series KVM switches

The KVM Switch CAT-32 is compatible with most other brands of KVM switches using a port cascaded installation. To prevent any hotkey conflicts, please ensure that the KVM hotkeys of the other KVM switches used are not the same as those used on the KVM Switch CAT-32 IP. The KVM hotkeys of the KVM Switch CAT-32 IP can be configured via the OSD.

## 1.4. Product Features

- 32 UTP Cat.5/6 server ports in a narrow 1U, 19" rack mount design
- Dual console operation option: Local console connected by PS/2 and VGA plus a remote access slot for optional KVM over IP module
- Compatible with all commonly used operating systems
- Supports USB as well as PS/2 computers using the appropriate Computer Modules
- Hot Plug Support allows computers to be added or removed for maintenance without powering down the KVM switch or the computers
- High Quality Video – Supports display resolutions of up to 1920 x 1200 at the local console
- Supports up to 1280 x 1024 at the IP console, 1600 x 1200 in virtual desktop mode
- No Software Required - easy computer selection via the On Screen Display Menu or Keyboard Hot Keys
- Each computer can be individually named in the On Screen Display Menu
- Password log in protection for access to the KVM Switch, auto log out option
- SSL security and additional password protection for IP access users
- Auto Scan Mode with an adjustable scan time from 5~104 seconds for monitoring computers
- Keyboard status automatically restored when switching between computers
- Front panel LED indicators for easy status monitoring
- 2 Digit LED display indicates the cascaded KVM Switch number
- 32x RJ45 ports for UTP cables to connect to the servers with up to 100m distance each
- Separate built-in daisy chain port prevents the loss of any computer port when cascading

## 1.5. Package Contents

- No. 39632, (1) KVM Switch CAT-32
  - (2) Firmware upgrade cable
  - (3) Daisy Chain cable
  - (4) Power Adapter
  - (5) 19" Rackmount Kit
  - (6) User manuals (English, French, German, Italian)
- No. 39636, (1) KVM over IP Module for KVM Switch CAT-32 IP
  - (2) USB cable type A/Mini-B
  - (3) CD with Utilities & Manual (English)
  - (4) Printed Quick Start Guides (English, French, German, Italian)

## 1.6. Optional Cables and Accessories

The remote access KVM over IP module, LINDY No. 39636, can be installed at any time. (To install it into the KVM Switch CAT-32 ensure all connected computers are switched off or disconnected and the power supply is unplugged. Open the slot on the back of the KVM Switch and slide the module into the slot.)

The local monitor, PS/2 mouse and PS/2 keyboard is connected using their standard cables.

To connect each individual computer to the switch, Cat.5/6 computer modules are required. For USB or PS/2 computers different modules have to be used as listed below:

- For PS/2 computers: Cat.5/6 Computer module PS/2 & VGA, LINDY No. 39633
- For USB computers: Cat.5/6 Computer module USB & VGA, LINDY No. 39634

A Cat.5e or 6 UTP cable of appropriate length (max. 100m) is required to connect the KVM Switch to the computer modules. These cables are available from LINDY in several different colors and lengths from 0.3m up to 100m. We don't recommend using shielded FTP/STP cables. Please find a small overview below:

### UTP Cat.5e

0.5m	1m	2m	3m	5m	7.5m	10m	15m	20m	30m
45961	45962	45963	45964	45965	45966	45967	45968	45969	45970

40m	50m	60m	70m	80m	90m	100m
45971	45972	44733	45974	44735	44736	45977

### UTP Cat.6

0.5m	1m	2m	3m	5m	7.5m	10m	15m	20m	30m
45771	45772	45773	45774	45775	45776	45777	45778	45779	45780

### Daisy Chain Cable

A short Daisy Chain Cable is included to cascade KVM switches with each other. Longer cables are available from LINDY: No. 39637 (1m) and No.39638 (2m).

To reach even longer distances several 2m cables can be chained together.

# Section 2

## Hardware Installation

### 2.1. Hardware Installation Guide

Before you start please verify that all parts are included according to the package contents listed previously.

Please prepare the required amount of KVM Computer Access Modules and UTP cables to connect to your computers/servers.

If you want to install the KVM Switch in a 19" server rack please attach the enclosed 19" rack mount brackets using the screws provided.

**If you intend to install the optional KVM over IP module then please install it into the module slot before you connect the servers and the power supply to the KVM Switch. You may also wish to attach one of the information labels supplied with the KVM over IP module to the back (or the front) of the KVM Switch so that you can easily locate the IP modules MAC address.**

In addition to the computers/servers to be connected you will need a PS/2 keyboard, monitor and PS/2 mouse to use as a local console.

#### Cascading / Daisy chaining of multiple KVM Switches

You can integrate up to 8 KVM Switches in one KVM daisy chained installation with up to a maximum of 256 attached computers.

To connect an additional slave KVM Switch to the MASTER (or previous) KVM switch use a standard daisy chain KVM cable as mentioned above. Connect it to the **Daisy Chain OUT** port of the **MASTER** KVM switch and to the **Daisy Chain IN** port of the first slave KVM switch. To connect the second slave KVM switch connect the **Daisy Chain OUT** port of the **first slave** KVM switch to the **Daisy Chain IN** port of the second slave KVM switch. Repeat this step up to a maximum of 8 KVM switches with a maximum of 256 servers.

1. Switch off all the computers to be attached.
2. Connect the keyboard, monitor and mouse directly to the ports of the LINDY KVM Switch labelled **Local Console**.
3. Now connect the servers and computers to the ports labelled 1 to 32 using UTP cable of appropriate length and an appropriate Computer Access Module.
4. Attach the power supply to the KVM Switch. Switch on your monitor.

**To set up and configure the KVM over IP remote access modules please refer to section 4 of this user manual.**

**You may also refer to the printed Quick Start Guide supplied with the KVM over IP module.**

# Section 3

## KVM Switch Operation

### 3.1. KVM Switch Operation

**Please Note:** Your monitor will only display one computer signal at any one time. All keyboard and mouse commands are sent to this computer as shown on the monitor.

**When the computer connected to the currently selected port is not switched on, or is in sleep mode, the monitor will not display any signal.**

#### 3.1.1. Password Security

The KVM Switch CAT-32 IP has a single user password protection with auto logout security.

The additional security features for the KVM over IP user are based on SSL and additionally KVM encrypted connections with a further level of password login. Details can be found in section 5, KVM over IP module.

#### 3.1.2. Hot Plug Support

The KVM Switch supports a "Hot Plug" function for easy addition or removal of computers.

##### PS/2 computer modules

If a computer is already running and its PS/2 interface has already been initialized, it is not required to turn off the computer. Simply hot-plug the PS/2 computer module to the computer. Always connect the PS/2 mouse port first to allow the correct initialization sequence! If the PS/2 ports of the computer haven't been initialized during boot up it may however be necessary to turn off the computer before connecting the PS/2 computer module so the OS can initialize the PS/2 ports during boot up.

**Please note:** Some Operating Systems including certain Unix versions may be unable to support the "Hot Plugging" function. If you "Hot Plug" when using this kind of O.S., it may cause unpredictable operation and may even shut down the computer.

##### USB computer modules

The USB and VGA interface is hot pluggable on most OS and computer systems. Therefore you may connect and disconnect USB computer modules at any time. Connect the computer modules to the KVM Switch using UTP Cat.5e/6 cables of appropriate length. In most cases standard patch cable UTP Cat.5e or 6 can be used without any problems. For best video results at very large distances and high resolutions UTP Cat.6 solid core cable may be used to improve video quality and distance. Shielded FTP/STP is not recommended. After the computers are connected and powered up you can access them from the KVM Switch CAT-32.

### 3.1.3. Computer / Port Selection

You can select the computer you want to access in one of two different ways:

- Keyboard hotkey selection
- On screen display menu selection

### 3.1.4. Illuminated front display

The front display has a two digit display to show the number of the KVM switch in the cascade: 01: Master, 02: first slave, 03: second slave. In addition one LED per Port shows the status of the connected port:

**GREEN (solid):** the computer on this port is powered (switched on or soft off with 5V active)

**GREEN (blinking/flickering):** this port is currently selected, displayed on the monitor, and keyboard/mouse commands are sent to the computer attached to this port.

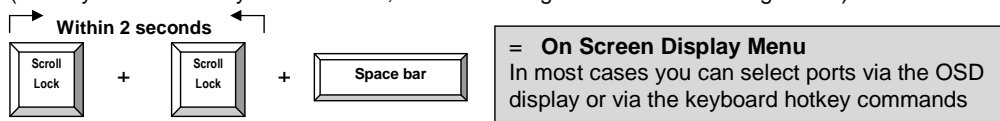
**Dark:** No computer connected or computer not powered up / no 5V signal active

One red Power LED near the bank display shows if the KVM Switch is powered up.

## 3.2. Keyboard Hotkey Selection and OSD Commands

Press the following key combination to enter the OSD menu:

(Factory Default Hotkey is Scroll Lock; it can be changed via the OSD configuration)



With a small delay the OSD pops up on your monitor and you can use the cursor keys to navigate through the OSD and select functions by pressing the Return key.

Alternatively, instead of waiting for the OSD, you can press the initial Scroll Lock hotkey twice and add further direct keyboard hotkey commands within 2 seconds after the initial hotkey to switch computer ports directly or change the KVM Switch CAT-32 settings etc.

Further available direct hotkey commands:

Command	Action
↑ (Cursor up) / ↓ (Cursor down)	Select next higher/lower port
Page Up / Page Down	Select next higher/lower bank/KVM switch
H + { Scroll / Num / Caps / ESC / F12 }	Change primary hotkey
0101 ..... 0832	Bank + port number direct selection
T	OSD port info screen on/off
Z	Remote console on/disabled
S	Start Autoscan

## 3.3. On Screen Display Menu (OSD)

The On Screen Display menu provides a lot of information about the switch configuration and the attached computers, and offers advanced administration and full KVM Switch control to the user.

Activate the OSD by the hotkey sequence:

Scroll Lock + Scroll Lock + space bar

### Main OSD Menu

Select computer/port: use **Up/Down Arrow** key to navigate, **Page Up/Page Down** to scroll page, hit **Enter** to select.

Edit computer name: just hit **Insert** to edit and **Enter** to confirm.

**F2: Save** - Save all modifications you have made.

When pressing F2, you will see the message-- "Saving parameters" for confirmation.

**F1: Setup** - rotate through **Main/ Video Setting/ Setup/ Status OSD menu pages**



Main OSD Menu

### Setup OSD Menu

**Auto logout:** specify the timeout before an auto-logout (00~99 min, +1 min) is performed

**OSD Timeout:** specify timeout for OSD menu remaining on screen (00~99 sec, +5 sec)

**AutoScan period:** Specify the delay time for auto scan (00~99 sec, +5 sec)

**Title bar:** Specify the title bar position (Left/Right/Disable)

**Hotkey:** specify the hotkey preceding sequence (SCROLL LOCK, CAPS, F12 or NUM LOCK)

**Password:** Enable/Disable password protection

**Enable /Disable Remote Console:** Toggle the remote console On/Off. If the remote console is in OFF state, a message will remind you appearing under the OSD title bar, **Remote control disabled** Always press F2 to save any changes!



F1 Setup OSD Menu

### Video setting Menu

Allows you to adjust video settings individually for every port:

**Gain:** specify level of gain. (00 ~ 50)

**Equ:** specify level of equalization. (00 ~ 50)

Go to Main/Video setting, and then begin to adjust the video parameters such as gain/equalization. Start with equalization to adjust the sharpness and shadows followed by gain for the brightness. It may be necessary to try several different settings and combinations to achieve the best display. Always press F2 to save any changes!



Video Setting Main Menu

**Status Menu**

This status page shows information for all daisy chained KVM Switches: Firmware version, KVM Switch PCB model and max. number of ports. Select one bank and press Enter to access the status pages of the Cat.5 computer modules connected to that KVM Switch.

**Computer Module Status Submenu**

Use this page to check the firmware version of the Cat.5 Computer Modules attached to a selected KVM Switch (i.e. 120208 shown here is the FW version of the KVM Switch), and perform manual FW upgrades. To do a manual FW upgrade of individual Cat.5 computer modules, just select the module to be upgraded and press Enter to confirm the automatic upgrade. During the upgrade process a download bar will appear indicating the progress of the upgrade. In addition you can alternatively press F4 to toggle between manual and auto (for all Cat.5 modules connected to this KVM Switch) upgrade mode. More detailed information is provided with the Firmware upgrade files.

**Firmware Update**

Use the supplied Firmware update cable to connect between the Daisy Chain In port of the KVM switch and the DB9 RS-232 port on your computer.

**3.4. Troubleshooting**

Before calling technical support, please try the following steps for easy troubleshooting.

**Q1. My keyboard and/or mouse are locked up. What can I do for troubleshooting without rebooting the computer and/or KVM?**

A1. First, unplug the console keyboard and mouse for a few seconds and plug them back in. This will re-initialize the console keyboard and mouse, in case an initialization failure of the console keyboard and mouse has happened. If this doesn't work, unplug the computer modules PS/2 or USB connections from the computer for few seconds and plug it in again - alternatively plug the USB connector into to a different USB port. If it is PS2, always connect the mouse connection first, then the keyboard connection. This should bring back the computer module if only re-initialization is required. If any of the above does not help then you may have to reboot the computer for a complete reset of the computer keyboard and mouse.

**Q2. My monitor stays dark.**

A2. Please check if the computer you want to access is in Standby or power save mode with the monitor switched off. If so please wake up the computer in the usual way.

The contact information for the LINDY technical support teams can be found on the LINDY website for each country.

**Cat5 OSD KVM**

	Ver.	Model	
01	020408	UKS-0132	08
02	020408	UKS-0132	16
03	020408	UKS-0132	08
04	020408	UKS-0132	16
05	020408	UKS-0132	08
06	020408	UKS-0132	32
07	020408	UKS-0132	32
08	260308	UKS-0132	32

F1 Main menu    ESC Quit  
Pg Up Prev status page  
Pg Dn Next status page

Status Menu

**Cat5 OSD KVM**

**Dongle status**

	Ver.	Model	
01	-	-	120208
02	-	-	
03	-	-	
04	-	-	
05	-	-	
06	-	-	
07	-	-	
08	-	-	

Enter again to confirm

Esc Backward    F4 AutoUpg  
Enter Upgrade  
Pg Dn Next page  
Pg Up Prev page

Computer Module Status Submenu

**Section 4**

Intentionally left empty  
For future use

# Section 5

## IP Access Configuration & Operation



### 5.0.1. KVM over IP Access Features

The IP access module provides remote KVM over IP access to the KVM switch CAT-32. It converts all keyboard video and mouse signals and sends them as TCP/IP signals over your LAN/WAN connection. The KVM switch CAT-32 IP may be accessed from any computer connected to your network and provides full KVM access including BIOS level access to all the connected computers.

Please note that KVM over IP does not operate in a “real time” environment and that some degree of time delay will occur due to limiting factors such as available bandwidth and network traffic.

The KVM over IP Access module can be accessed via a simple web browser and via dedicated software tools included with the product. It uses secure encrypted sessions and password authentication protocols.

Please note that the conversion of video, mouse and keyboard signals requires a certain amount of CPU processing time. Transporting large amounts of data over TCP/IP requires a high bandwidth connection. Limited bandwidth may restrict or limit the possible screen resolutions and colour depths which can be transmitted over your LAN / WAN.

A connection which exhibits limited bandwidth will result in slower mouse reaction and cursor control. Also the available screen resolution, colour depth and refresh rates will also be affected. Ensure the connection you are using provides adequate bandwidth, some adjustment of screen resolution, colour depth and mouse cursor control may have to be made for satisfactory operation.

### 5.0.2 KVM over IP Access Module Installation

Before you install the IP Access module into the KVM switch ensure all connected computers are switched off and the power supply is unplugged. Proceed to unscrew and remove the small metal cover on rear of the KVM switch. Carefully slide the module into the slot and secure in place with the screw previously removed.

You may now proceed to power up all connected equipment and check for correct operation.

**For the remainder of this manual the CAT-32 KVM switch with installed KVM over IP Module will be referred to as CAT-32 IP.**

### 5.1. Configuration

The CAT-32 IP's communication interfaces are all based on TCP/IP. The switch comes pre-configured with the following IP configuration shown here:

Parameter	Value
IP auto configuration	DHCP
IP-Address	-
Net-mask	255.255.255.0
Default-Gateway	none

**Note:** If the DHCP connection fails on boot-up, the CAT-32 IP will not be assigned an IP address.

If this initial configuration does not meet your requirements, the following section describes the configuration that is necessary to access the CAT-32 IP for the first time.

#### Initial Configuration via a DHCP Server

By default, the CAT-32 IP will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it will provide a valid IP address, gateway address and subnet mask. If a DHCP server is not available then you will need to assign a fixed IP assignment to the MAC address of the IP Access Module. You can find the MAC address details on the printed label on the underside of the IP Access module.

Before you connect the device to your local subnet, be sure to complete the corresponding configuration using the setup tool supplied on the CD ROM. Follow the procedure described on the next page (**Section 5.2**)

#### Initial Configuration via a Serial Console

The CAT-32 IP has a serial line interface (host side) for connecting a serial terminal. This connector is compliant with the RS232 serial line standard. The serial line has to be configured with the parameters given in this table:

Parameter	Value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

When configuring with a serial terminal, reset the CAT-32 IP and immediately press the **ESC** key. You will see some device information and a “=>” prompt. Type **config** and press the **Enter** key. Wait a few seconds for the configuration information to appear.

As you proceed, the following questions will appear on the screen. To accept the default values (shown in square brackets below) press the **Enter** key.

**IP auto configuration (non/dhcp/bootp) [dhcp]:**  
**IP [192.168.1.22]:**  
**Net mask [255.255.255.0]:**  
**Gateway (0.0.0.0 for none) [0.0.0.0]:**

## 5.2 CAT-32 IP Setup Tool

### MAC Address Detection

Connect the CAT-32 IP to your computer either via a local network, or via USB. If you use a USB connection Windows will detect the CAT-32 IP as a '**Removable Disk**' and an appropriate drive letter will be assigned.



Start the setup tool from the CD ROM.

A window opens as shown below:

On the upper left corner, the MAC address of the CAT-32 IP is displayed. To re-detect the MAC address, press the **Refresh Devices** button. The displayed MAC address should correspond to the printed address shown on the label on the base of the IP module.

On the lower right corner of the window, there are two buttons: **Query Device** and **Setup Device**. Press the **Query Device** button to display the preconfigured values of the network configuration. The values are displayed in the text fields located above. If necessary, adjust the network settings to your needs. To save the changes enter a user login and a password (**see Authentication, below**) and then press the **Setup Device** button.

### Authentication

To adjust the authentication settings, enter your login as a super user and change your password.

#### Super user login

Enter the login name of the super user. The initial value is "**super**". All of the characters are lower case.

#### Super user password

Enter the current password for the super user. This initial value is "**pass**". All of the characters are lower case.

#### New super user password

Enter the new password for the super user.

#### New password (confirm)

Re-type the new password for the super user.

To close the window and accept the changes, press the **OK** button, otherwise press the **Cancel** button.

### IP Auto Configuration

With this option, you can specify whether the CAT-32 IP should obtain its network settings from a DHCP or BOOTP server. From the drop down list select either **DHCP** or **BOOTP**. If you select **NONE**, the IP auto configuration is disabled and you should manually input the following network settings:

#### IP address

The IP address the CAT-32 IP uses.

#### Net mask

The net mask of the connected IP subnet.

#### Gateway address

The IP address of the default router for the connected IP subnet. If you do not have a default router, enter **0.0.0.0**.

### 5.3. Keyboard, Mouse and Video Configuration

Between the CAT-32 IP and the host, there are two interfaces available for transmitting keyboard and mouse data: USB and PS/2. The correct operation of the remote mouse depends on several settings which will be discussed in the following subsections and section 5.7.4.

#### CAT-32 IP Keyboard Settings

The CAT-32 IP settings for the host's keyboard type have to be correct in order to make the remote keyboard work properly. The settings can be checked using the CAT-32 IP front-end, please see section 5.7.4 for details of how to make changes to the keyboard settings.

#### Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The CAT-32 IP addresses this problem with an intelligent synchronization algorithm. There are two mouse modes available on the CAT-32 IP: **Auto mouse speed** and **Fixed mouse speed**.

##### Auto mouse speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. Speed detection is performed during mouse synchronization. If the mouse does not move correctly, there are two ways to re-synchronize the local and remote mouse:

**Fast Sync:** Fast synchronization is used to correct a temporary, but fixed skew. Choose this option using the Remote Console options menu or by pressing the mouse synchronization hotkey sequence - **[ALT] + [F12]**

**Intelligent Sync:** If the fast sync does not work correctly or the mouse settings have been changed on the host system, you can use the intelligent resynchronization option. This method can be accessed from the **Mouse Handling** sub menu of the Remote Console **Option** menu.

Intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function or manual correction in the Video Settings panel to setup the picture. **The Sync mouse button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization.** Usually pressing this button leads to a fast sync, except in situations where the KVM port or the video mode was recently changed.

**Tip:** When first started, if the local mouse pointer is not synchronized with the remote mouse pointer, click the **Auto Adjust Button** once. If the mouse is still not synchronized select **Intelligent Sync** from the **Mouse Handling** sub menu of the Remote Console **Option** menu.

##### Fixed mouse speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to 'n' pixel moves on the remote system. This parameter 'n' is adjustable. However, it should be noted that this works only when mouse acceleration is turned off on the remote system.

### Host System Mouse Settings

The host's operating system obtains various settings from the mouse driver.

**Note:** The following limitations do not apply when using USB mice and Windows 2000 and higher!

#### Special Mouse Driver

There are mouse drivers which influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

#### Windows XP Mouse Settings

If using Windows XP, disable the **enhance pointer precision** setting.

#### Active Desktop

If the Active Desktop feature of Microsoft Windows is enabled, do not use a plain background. Instead, use some kind of wallpaper. Alternatively, you could also disable the Active Desktop completely.

Navigate your mouse pointer into the upper left corner of the applet screen and move it back and forth slightly. In this way the mouse will be resynchronized. If re-synchronizing fails, disable mouse acceleration and repeat the procedure.

### Single and Double Mouse Mode

The information above applies to **Double Mouse Mode**, where both remote and local mouse pointers are visible and need to be synchronized. The CAT-32 IP also features another mode - **Single Mouse Mode**, where only the remote mouse pointer is visible. Activate this mode in the open Remote Console and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode, use the hotkey combination **[ALT] + [F12]** to free the captured local mouse pointer.

### Recommended Mouse Settings

For the different operating systems we can give the following advice...

#### MS Windows 2000/2003 (Professional and Server), XP, Vista,

In general, we recommend the use of a USB mouse. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed.

For XP, Vista, disable the option called **enhance pointer precision** or similar in the Control Panel.

#### SUN Solaris

Adjust the mouse settings either via **xset m 1** or use the CDE Control Panel to set the mouse to 1:1, no acceleration. As an alternative you may also use the Single Mouse Mode.

#### MAC OS X

We recommend using the Single Mouse Mode.

### Video Modes

The CAT-32 IP switch recognizes a limited number of common video modes. When running X11 on the host system, please do not use any custom mode lines with special video modes. If you do, the CAT-32 IP switch may not be able to detect them. We recommend using any of the standard VESA video modes instead.

## 5.4. Usage

### Prerequisites

The CAT-32 IP features an embedded operating system offering a variety of standardized interfaces. This section will describe these interfaces, and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family.

The following interfaces are supported:

#### Telnet

A standard Telnet client can be used to access an arbitrary device connected to the CAT-32 IP's serial port via a terminal.

#### HTTP/HTTPS

Full access is provided by the embedded web server. The CAT-32 IP switch environment can be entirely managed using a standard web browser. You can access the CAT-32 IP using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

The primary interface of the CAT-32 IP is the HTTP interface. This is covered extensively in this section. Other interfaces are addressed in the relevant subsections.

In order to use the Remote Console window of your managed host system, the browser must feature Java Runtime Environment version 1.1 or higher support. If the browser has no Java support (such as on a small handheld device), you can still maintain your remote host system using the administration forms displayed by the browser itself.

**Important: We recommend you install the latest version of Sun's Java Virtual Machine which can be downloaded from the following web site:**  
**[www.java.com](http://www.java.com)**

For a non-secure connection to the CAT-32 IP, we recommend the following browsers:

- Microsoft Internet Explorer version 6.0 or higher
- Netscape Navigator 7.0 or Mozilla 1.6

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of at least 128 Bit. Some older browsers do not have a strong 128 Bit encryption algorithm.

## 5.5. Logging In

### Login to the CAT-32 IP

Launch your web browser. Direct it to the address of your CAT-32 IP which you configured during the installation process. The address used might be a plain IP address or a host and domain name if you have given your CAT-32 IP switch a symbolic name in the DNS.

**Example:** Type the following in the address line of your browser when establishing an unsecured connection:

**http://<IP address of CAT-32 IP>**

When using a secure connection, type in:

**https://<IP address of CAT-32 IP>**

This will lead you to the CAT-32 IP login page as shown below:

The CAT-32 IP has a built-in super user account that has all the permissions enabled to administrate your CAT-32 IP switch:

Login name	super (factory default)
Password	pass (factory default)

**Please note:** Your web browser has to accept cookies, or else login is not possible.

**Note:** The user "super" is not allowed to login via the serial interface of the IP-KVM switch.

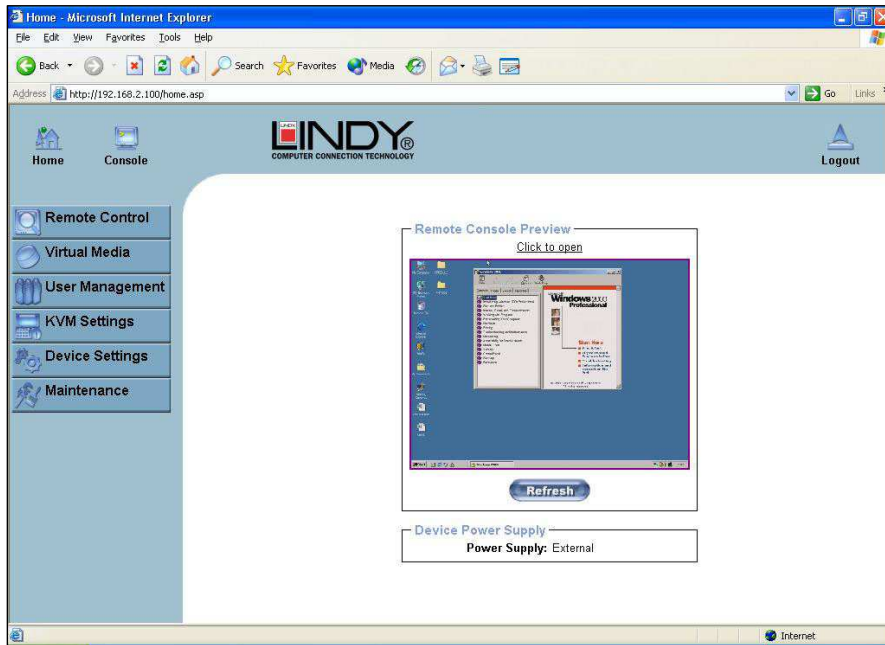
Please make sure you change the super user password immediately after you have installed and accessed your CAT-32 IP for the first time. Not changing the password for the super user is a severe security risk and could result in unauthorized access to the switch and to the host system(s) to which it is connected.

#### Technological progress

The KVM over IP Module, its software and firmware are subject to technological progress and are being continuously upgraded accordingly. Therefore minor changes compared to the descriptions in this manual may be found, especially for the design of the screens and menus.

## 5.6. Navigation

Once logged into the CAT-32 IP successfully, the main page appears. This page consists of three parts; each of them contains specific information. The buttons in the upper area allow you to navigate within the front end. The lower left area contains a navigation bar and allows you to switch between the different sections of the CAT-32 IP. Within the main area, task-specific information is displayed.



Return to the main page of the CAT-32 IP



Logout from the CAT-32 IP



Access the Remote Console

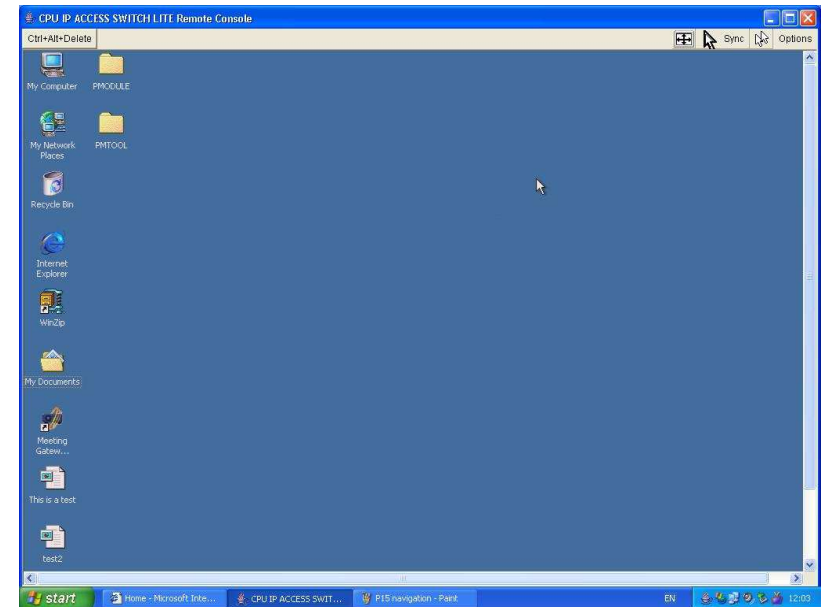
The Remote Console is the redirected screen, keyboard and mouse of the remote host system that the CAT-32 IP switch controls. Selecting this button opens the **Remote Console Main Window**.

The Remote Console window is a Java Applet that establishes its own TCP connection to the CAT-32 IP. The protocol that runs over this connection is neither HTTP nor HTTPS, but RFB (Remote Frame Buffer Protocol). RFB needs to establish a connection to port number 443. Your local network environment has to allow this connection to be made, i.e. your firewall and, if you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

If the CAT-32 IP is connected to your local network environment and your connection to the Internet is available using a proxy server only, without NAT being configured, the Remote Console is very unlikely to be able to establish a connection. This is because today's web proxies are not capable of relaying the RFB protocol.

If you experience problems, please consult your network administrator in order to provide an appropriate network environment.

### Remote Console Main Window



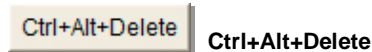
Starting the Remote Console opens an additional window. It displays the screen content of the currently selected computer connected to the CAT-32 IP. The Remote Console will behave in exactly the same way as if you were using the local console. You can use the CAT-32 IP keyboard hotkeys to switch between computers, activate the OSD etc., as well as control the currently selected computer. However, be aware that the host system will react to keyboard and mouse actions with a slight delay.

**Note:** Your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system and your host system uses a US English keyboard layout for instance, some special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

### Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the state of the Remote Console and influence the local Remote Console settings. A description for each control follows.



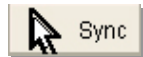
**Ctrl+Alt+Delete**

Sends the 'Control Alt Delete' key combination to the remote system



**Auto Adjust button**

If the video display is poor quality or distorted in some way, click this button and wait a few seconds while the CAT-32 IP tries to adjust itself for the best possible video quality.



**Sync mouse**

Activates the mouse synchronization process. Choose this option in order to synchronize the local AND remote mouse cursors. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.



**Single/Double mouse mode**

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible) Single mouse mode is only available if using SUN JVM 1.3 or higher.

**Tip:** When in single mouse mode use the hotkey combination [ALT] + [F12] to release mouse control and access the menus etc.

### Options

#### Options

Opens the Options menu. A short description of the each of the options follows:

#### Monitor Only

Toggles the 'Monitor only' filter on or off. If the filter is switched on, no remote console interaction is possible but monitoring is.

#### Exclusive Access

If a user has the appropriate permission, he can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access, or logs off.



A change in the access mode is also visible in the status line indicated by this icon.

#### Scaling

Allows you to scale down the Remote Console. You can still use both mouse and keyboard; however the scaling algorithm will not preserve all display details.

#### Mouse Handling

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse pointer.

##### Fast Sync

The fast synchronization is used to correct a temporary, but fixed skew.

##### Intelligent Sync

Use this option if the fast sync does not work or the mouse settings have been changed on the host system

**Note:** This method takes more time than fast sync and requires a correctly adjusted picture. Use the auto adjustment function or the manual correction in the Video Settings panel to setup the picture.

#### Local Cursor

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine; a version of 1.2 or higher offers the full list.

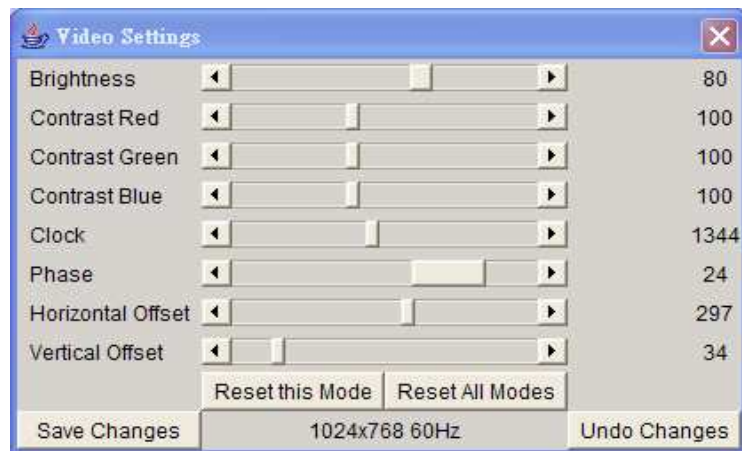
#### Video Settings

Opens a panel for changing the CAT-32 IP video settings. The CAT-32 IP features two different dialogs, which influence the video settings:

#### Video Settings in the KVM section in the front end menu:

The Noise Filter option defines how the CAT-32 IP reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.



**Video Settings through the remote console:****Brightness**

Controls the brightness of the picture

**Contrast**

Controls the contrast of the picture

**Clock**

Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjunction with the auto adjustment procedure should be adequate for most common configurations. If the picture quality is still bad after auto adjustment you may change this setting together with the sampling phase to achieve a better quality.

**Phase**

Defines the phase for video sampling; used to control the display quality together with the setting for sampling clock.

**Horizontal Offset**

Use the left and right buttons to move the picture in a horizontal direction

**Vertical Offset**

Use the left and right buttons to move the picture in a vertical direction

**Reset this Mode**

Reset mode specific settings to the factory-made defaults.

**Reset all Modes**

Reset all settings to the factory-made defaults.

**Save Changes**

Save changes permanently

**Undo Changes**

Restore last settings

**Soft Keyboard**

Opens up the sub-menu for the Soft-Keyboard:

**Show**

Pops up the Soft-Keyboard. The Soft-Keyboard is necessary in case your host system runs a completely different language and country mapping than your administration machine.

**Mapping**

Used for choosing the language and country mapping of the Soft-Keyboard.

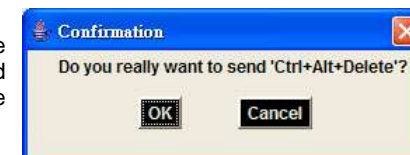
**Local Keyboard**

Used to change the language mapping of your browser running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular KVM and your browser settings this is not always possible. A typical example is a German localized system that uses a US-English keyboard mapping. In this case you must manually change the local keyboard setting to the correct language.

**Hotkeys**

Opens a list of previously defined hotkeys. Choose one entry; the command will be sent to the host system.

A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Select **OK** to perform the command on the remote host.



## Remote Console Status Line

### Status line

Shows both console and the connection state. The size of the remote screen is displayed. The example below was taken from a Remote Console with a resolution of 1024 x 768 pixels. The value in brackets describes the connection to the Remote Console. **Norm** means a standard connection without encryption, **SSL** indicates a secure connection.



Furthermore, both the incoming (**In** :) and the outgoing (**Out** :) network traffic are visible (in kb/s). If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

In: 0 B/s Out: 0 B/s

For more information about **Monitor Only** and **Exclusive Access** settings, see the relevant section 5.7.4.

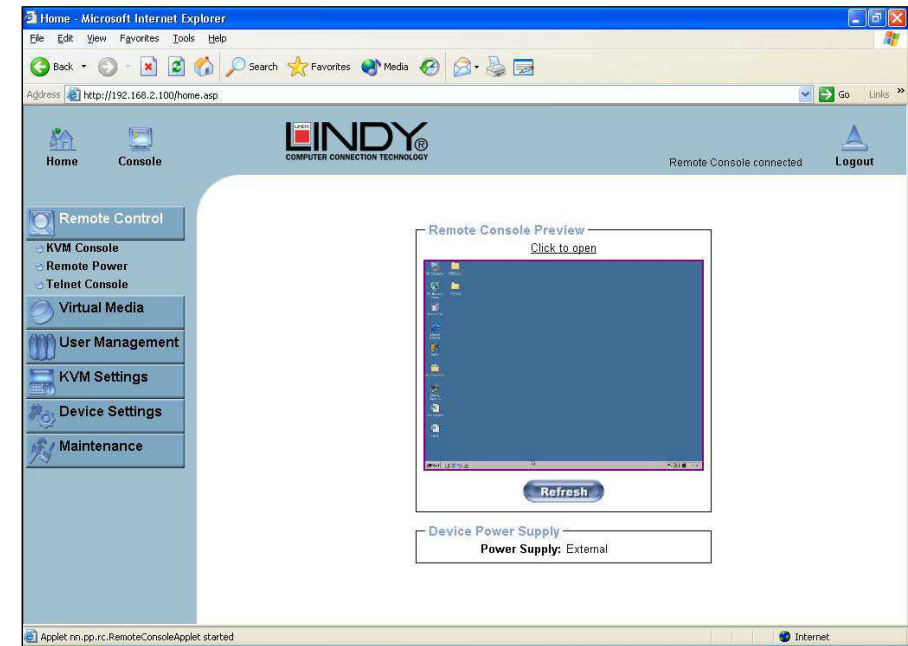
## 5.7. Menu Options

### Technological progress

The KVM over IP Module and its software and firmware are subject to technological progress and are being continuously upgraded accordingly. Therefore minor changes compared to the descriptions in this manual may be found, especially for the design of the screens and menus.

### 5.7.1. Remote Control

#### KVM Console



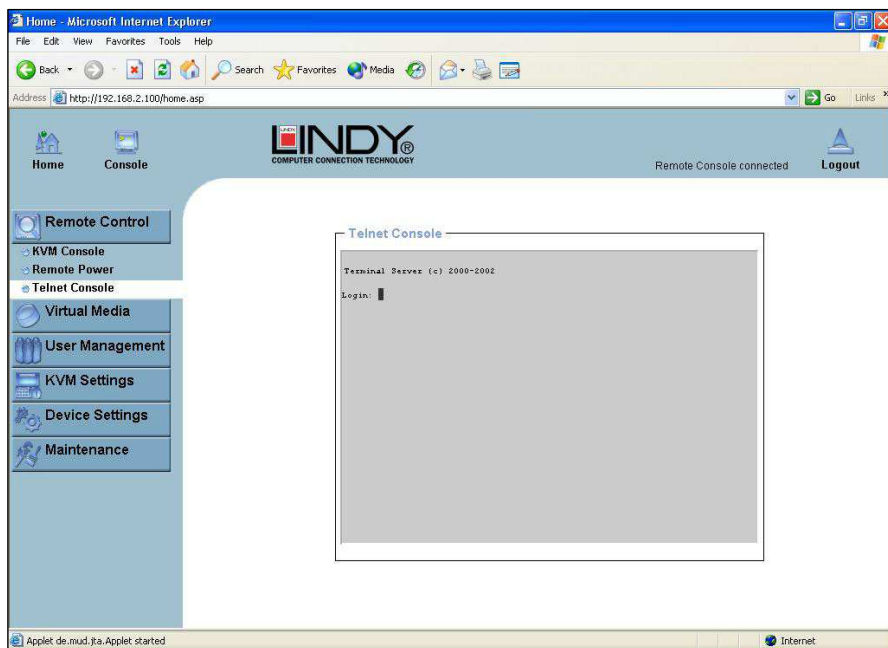
To open the KVM console, click either the menu entry on the left or on the console picture on the right. To refresh the picture, click on the **Refresh** button.

#### Remote Power

Future firmware updates will allow you to control external RS232 controlled power control distribution units. Please contact LINDY for further information regarding compatibility, connection and configuration of both LINDY and third party power control distribution units. Should you wish to connect a remote power outlet then LINDY would recommend you to use IP managed power strips that can be found in the network section of the LINDY website, i.e. LINDY No. 32657, 32658, 32656, 32654, 32653, 32414, 32415



## Telnet Console



The CAT-32 IP firmware features a Telnet server that enables a user to connect via a standard Telnet client. If the Telnet program is using a VT 100, VT 102 or VT 220 terminal or appropriate emulation, it is even possible to perform a console redirection, as long as the CAT-32 IP host is using a text mode screen resolution.

Connecting to the CAT-32 IP is done as usual and as required by the Telnet client, for instance in a UNIX shell:

```
telnet 192.168.1.22
```

Replace the IP address by the one that is actually assigned to the CAT-32 IP. This will prompt for the username and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means the user management of the Telnet interface is entirely controlled with the appropriate functions of the web interface.

Once you have successfully logged into the CAT-32 IP a command line will be presented and you can enter management commands directly.

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were made accordingly). All inputs are redirected to the device on serial port 1 and its answers are displayed on the Telnet interface.

The following list shows the command mode syntax and usage.

### Help

Displays the list of possible commands

### Cls

Clears the screen

### Quit

Exits the current session and disconnects from the client

### Version

Displays the release information

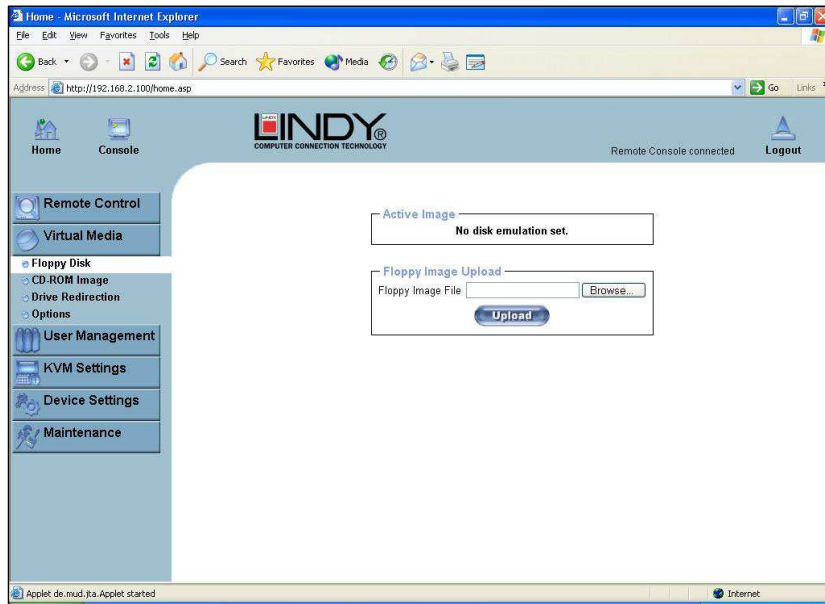
### Terminal

Starts the terminal pass-through mode for the serial port. The key sequence 'esc exit' switches back to the command mode.

### 5.7.2. Virtual Media

One of the computers connected to the CAT-32 IP can also be set up for remote mass storage via a USB connection. Files can be uploaded to the switch, which the host computer 'sees' as virtual drives. This means the remote operator can remotely install software, drivers etc. without the need to be sat in front of the host computer.

#### Floppy Disk



Follow the steps below to upload a virtual floppy image to the CAT-32 IP and create a virtual floppy drive on the host system.

#### Create a Floppy Image

First, on your client PC you must create an image of your floppy disk which can be uploaded to the CAT-32 IP's built in memory.

#### UNIX and UNIX-like OS

To create an image file, make use of **dd**. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a floppy image file copy the contents of a floppy to a file. You can use the following command:

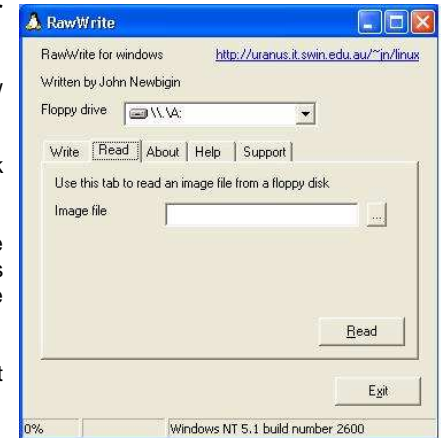
```
dd [ if=/dev/fd0 ] [ of=/tmp/floppy.image ]
```


**dd** reads the entire disc from the device **/dev/fd0** and saves the output in the specified output file **/tmp/floppy.image**. Adjust both parameters exactly to your needs (input device etc.)

#### Windows

Windows users should use the tool, **RawWrite for Windows**, which is included on the supplied CD.

Launch **RawWrite**, you will see the window opposite:



Insert your floppy disk into your floppy drive. Click the **Read** tab and then click on 

Select a name and destination for the floppy image file and click the **Read** button. As the image is written, you will see the progress as a percentage figure in the bottom left hand corner.

When the image has been written you can upload it to the CAT-32 IP.

#### Uploading a Floppy Image

Click the **Browse** button and navigate to the location of the image file, then click the **Upload** button.



After the image has uploaded you will see the dialog below:

**Floppy image uploaded successfully.**

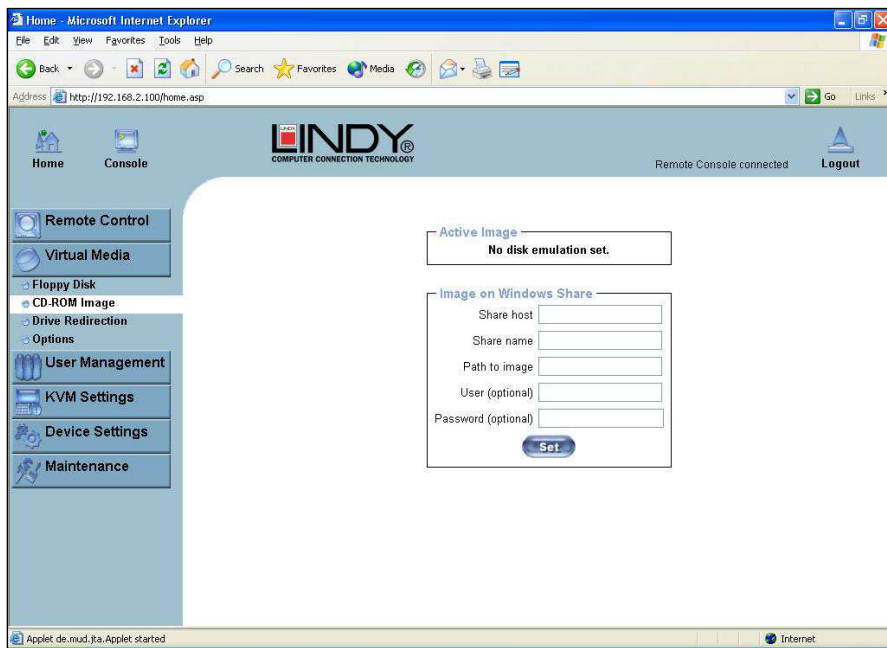


A virtual floppy drive will be installed on the host system and the image will be downloaded to the virtual floppy drive from the CAT-32 IP. You can access the virtual floppy drive in the same way you would a regular drive.

You can download the image from the CAT-32 IP to your remote system by clicking the **Download** button.

Clicking **Discard** removes the virtual floppy image from the CAT-32 IP and from the hosts system.

## Create a CD-ROM/ISO Image



Follow the procedure below to create a CD-ROM image which can be accessed by the host system via the CAT-32 IP. The image file must be an ISO file format!

First, on your client PC you must create an image of your CD which can be accessed by the host system.

### UNIX and UNIX-like OS

To create an image file, make use of **dd**. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a CD-ROM image file, copy the contents of the CD-ROM to a file. You can use the following command:

```
dd [ if=/dev/cdrom ] [ of=/tmp/cdrom.image ]
```

**dd** reads the entire disc from the device **/dev/cdrom**, and saves the output in the specified output file **/tmp/cdrom.image**. Adjust both parameters exactly to your needs (input device etc.).

### Windows

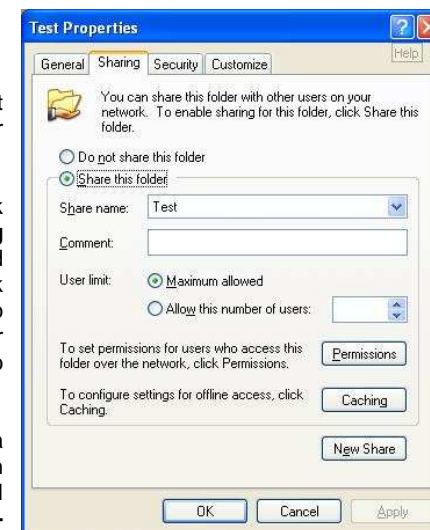
To create the image file, use your favorite CD imaging tool. Copy the whole contents of the disc into one single image file on your hard disk.

For example, with 'Nero' choose 'Copy and Backup'. Then, navigate to the 'Copy Disc' section. Select the CD ROM or DVD drive you would like to create an image from. Specify the filename of the image, and save the CD ROM content in that file.



Example:

1. Create a CD image and name it **image.iso**
2. Create a folder on your client PC and name it **Test**. Copy the file **image.iso** to the folder **Test**.
3. Now you need to 'share' this folder. Right click on the folder and select the option **Sharing and Security**. Select **Share this folder** and ensure the **Share Name** is set to **Test**. Click **Permissions** to set permissions for users who access this folder, according to your requirements. Click **Apply** then **OK** to complete.
4. Next you need to mount the image via a Windows Share. In the CAT-32 IP menu on the left hand side of the browser select **Virtual Media** and from the sub menu select **CD-ROM Image**.



5. Input the following parameters:

<b>Share host:</b>	Enter the IP address of your Console PC here (e.g. 192.168.2.103)
<b>Share name:</b>	Test (The share name of the previously created folder)
<b>Path to image:</b>	image.iso (the name of the CD image)
<b>User:</b>	super (Your user name, the default is super)
<b>Password:</b>	pass (Your password, the default is pass)

6. Click **Set**

7. You will see the dialog below detailing the active image:

**Image file set successfully**

**Active Image**

**CD-ROM Image**

**Image Host:** 192.168.2.104

**Image Share:** Test

**Image File with Path:** image.iso

**User name:** super

**Password:** not displayed

**Reactivate** **Unset**

**Image on Windows Share**

Share host

Share name

Path to image

User (optional)

Password (optional)

You must remove the current virtual disk to install a CD-ROM image.

8. Click **Reactivate**. Access the console window and you will see that another CD drive has been installed on the host computer. This is the virtual drive you have just set up. You can access the uploaded CD image as though it were a regular CD. Click **Unset** to remove the image.

### SAMBA

If you would like to access the share via SAMBA, SAMBA must be set up properly. You may either edit the SAMBA configuration file `/etc/samba/smb.conf`, or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

## Drive Redirection

Home - Microsoft Internet Explorer

Address http://192.168.2.100/home.asp

**INDY**  
COMPUTER CONNECTION TECHNOLOGY

Remote Console connected Logout

**Image file unset successfully**

**Active Image**

No disk emulation set.

**Drive Redirection**

Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.

To use this feature, you need the Drive Redirection Tool or the KVM Vision Viewer on your client machine. Please ask the vendor of CPU IP ACCESS SWITCH LITE how to get the tools.

☐ Disable Drive Redirection

☐ Force read-only connections

**Apply**

Remote Control

Virtual Media

Floppy Disk

CD-ROM Image

Drive Redirection

Options

User Management

KVM Settings

Device Settings

Maintenance

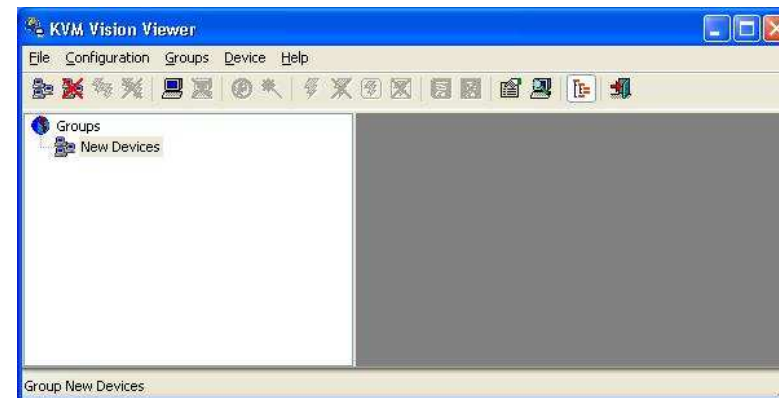
Applet de mud.f.a.Applet started

Internet


The Drive Redirection feature allows the host system to access the CD-Rom drives, hard drives, floppy drives etc. on your client PC.

To use this feature you need the Drive Redirection Tool which is part of the **KVM Vision Viewer** application included on the supplied CD.

1. To set up Drive Redirection, first install **KVM Vision Viewer**. After installation launch the application:

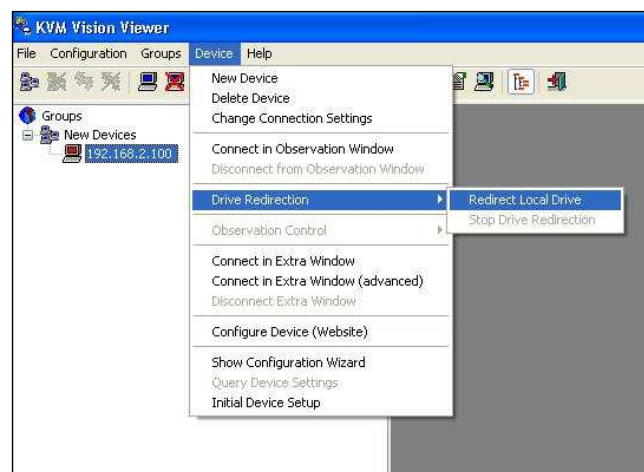




- Click on the **Search for new devices** icon -  The CAT-32 IP will be detected as an **Unconfigured device** and its MAC address will be displayed in the left panel. Double click on the MAC address to launch the **Device Configuration Wizard**.
- Follow the on-screen instructions. You will be asked to input your user name (default is **super**) and password (default is **pass**).



- Continue with the Wizard until the device is correctly configured. Once the configuration is complete, select **Redirect Local Drive** from the **Device** menu:



- Choose the drive you wish to redirect from the drop-down list. Enter your user name and password and click **OK**.

**Warning:** Please be aware that if **Allow Write Support** is selected, data on the shared media may be lost!



- Access the host computer from the Remote Console window. You will see that the redirected drive will now be shown in Windows Explorer:



#### IMPORTANT

- Drive Redirection is only possible with Windows 2000 and later versions.
- Drive Redirection works on a low SCSI level. The SCSI protocol cannot recognize partitions; therefore the whole drive selected will be shared instead of any particular partition.

#### Options

##### Virtual Media Options

- ☒ Disable USB Mass Storage if no image is loaded

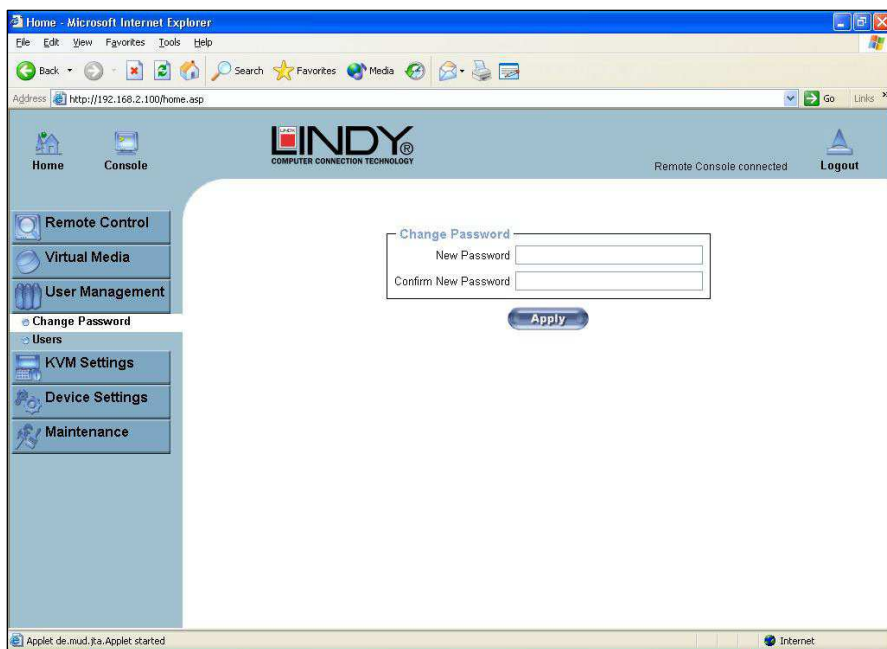
**Apply**

This option allows you to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. To set this option, press the button **Apply**.

### 5.7.3. User Management

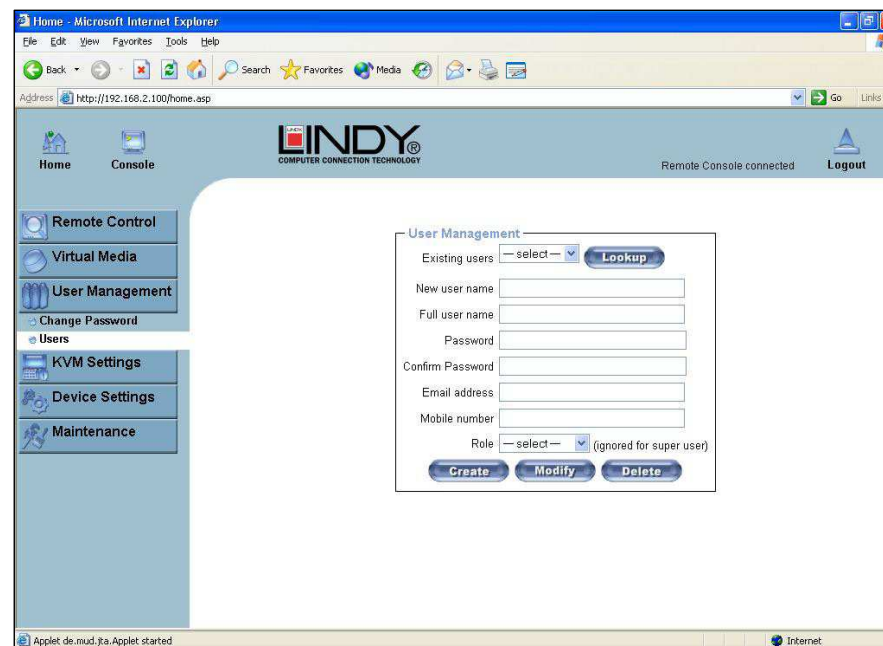
#### Change Password

To change your password, enter the new password in the upper entry field. Retype the password in the lower field. Click **Apply** to submit your changes.



### Users And Groups

The CAT-32 IP comes with 2 pre-configured user accounts that have fixed permissions. The **super** account has all possible rights to configure the device and to use all functions. The **user** account has only the permission to open and use the Remote Console. The default password for both accounts is "**pass**". Ensure you change the passwords as soon as you have installed and accessed the CAT-32 IP for the first time.



While the **user** account never sees the following options, the **super** account can change the name and password for both accounts.

#### Existing users

Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.

#### New User name

The new user name for the selected account.

#### Password

The password for the login name. It must be at least four characters long.

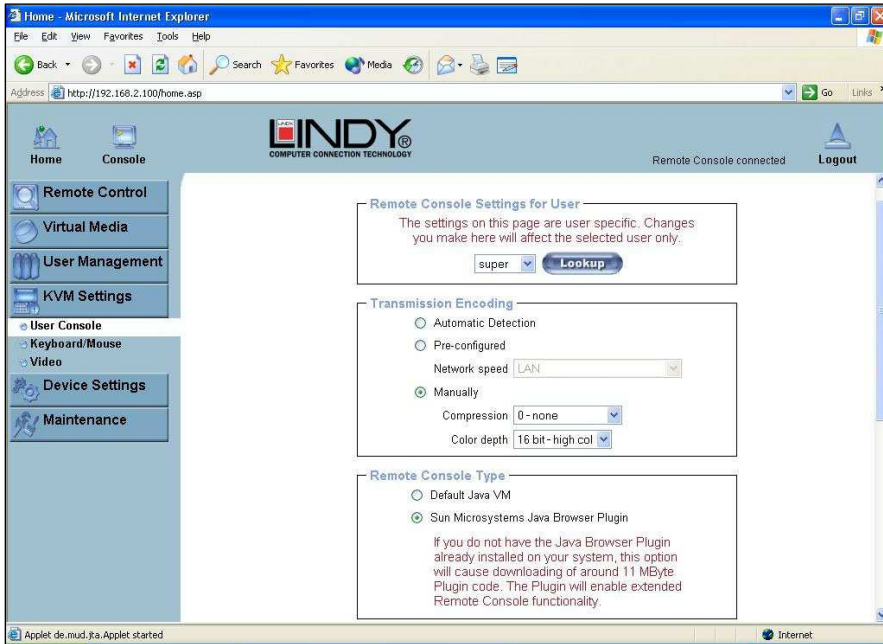
#### Confirm password

Confirmation of the above password.

### 5.7.4. KVM Settings

#### User Console

The following settings are user specific. This means the super user can customize these settings for individual users separately. Changing the settings for one user does not affect the settings for the other users.



#### User select Unit

This box displays the user ID for which the values are shown and for which the changes will take effect. You may change the settings of other users if you have the necessary access rights.

#### Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

#### Automatic detection

The encoding and the compression level are determined automatically from the available bandwidth and the current content of the video image.

#### Pre-configured

The pre-configured settings deliver the best result because of optimized adjustment of compression and colour depth for the indicated network speed.

#### Manually

Allows adjustment of both compression rate and colour depth individually. Depending on the selected compression rate the data stream between the CAT-32 IP and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used when several users are accessing the CAT-32 IP simultaneously.

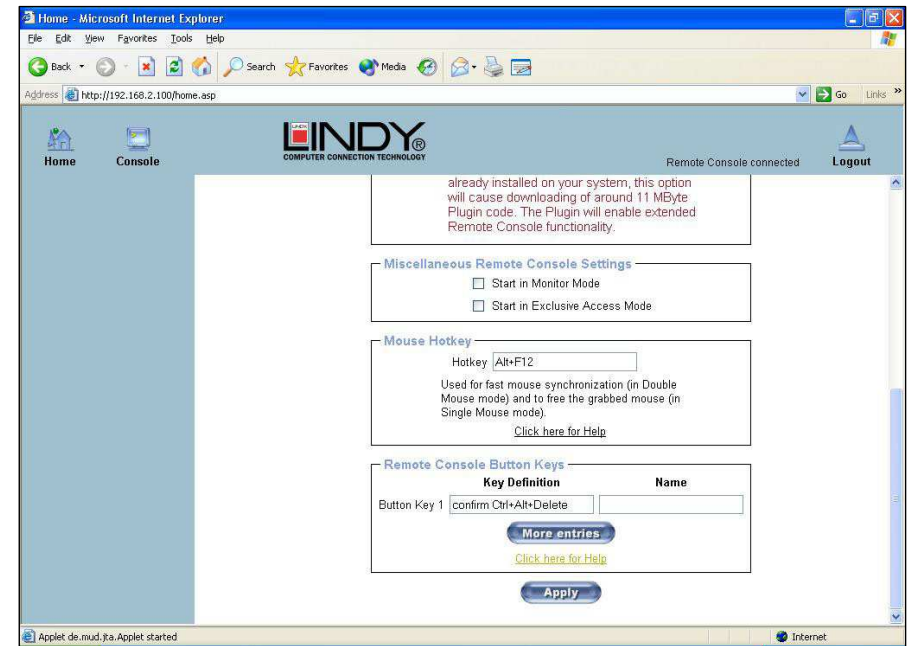
The standard colour depth is 16 bit (65536 colours). The other colour depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 bit colour depth. At lower bandwidths only 4 bit (16 colours) and 2 bit (4 grey scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 bit (16 grey scales). 1 Bit colour depth (black/white) should only be used for extremely slow network connections.

#### Remote Console Type

Specifies, which Remote Console Viewer to use.

#### Default Java-VM

Uses the default Java Virtual Machine of your Browser. This may be the Microsoft JVM for Internet Explorer or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).



### Sun Microsystems Java Browser Plug-in

Instructs the web browser of your administration system to use Sun's JVM. The JVM in the browser is used to run the code for the Remote Console window which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the appropriate dialogs with **yes**. The download size is around 11MB. The advantage of downloading Sun's JVM is in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for Sun JVM versions and offers wider range of functionality when run with JVM.

### Miscellaneous Remote Console Settings

**Start in Monitor Mode** Sets the initial value for the monitor mode. By default the monitor mode is off. In case you switch it on, the Remote Console window will be started in a read only mode.

**Start in Exclusive Access Mode** Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

### Mouse hotkey

Allows the user to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console or is used to leave the single mouse mode.

### Remote Console Button Keys

This allows simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are **Control+Alt+Delete** in Windows and DOS, which is always caught, or **Control+Backspace** on Linux for terminating the X-Server. The syntax to define a new Button Key is as follows:

**[confirm] <keycode>[+|-[\*]<keycode>]\***

**confirm** requests confirmation by a dialog box before the key strokes will be sent to the remote host.

**keycode** is the key to be sent. Multiple key codes can be joined with a plus, or a minus sign. The plus sign builds key combinations; all keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So the minus sign builds single, separate key presses and releases. The star inserts a pause with duration of 100 milliseconds.

### Keyboard/Mouse



### Host Interface

Enables the interface the mouse is connected to. You can choose between **Auto** for automatic detection, **USB** for a USB mouse, or **PS/2** for a PS/2 mouse.

**Note:** To use the USB and/or PS/2 interface you need the correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only, then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected **Auto** as host interface, then **USB** will be selected if available, otherwise it will revert to **PS/2**.

To enable USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

- the host BIOS must have USB keyboard support
- the USB cable must be connected or must be selected in the Host interface option

### PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between **Generic 101-Key PC** for a standard keyboard layout, **Generic 104-Key PC** for a standard keyboard layout extended by three additional windows keys, **Generic 106-Key PC** for a Japanese keyboard, and **Apple Macintosh** for the Apple Macintosh.



### USB Mouse Type

Enables USB mouse type. Choose between **MS Windows 2000 or newer** for MS Windows 2000 or Windows XP, or **Other Operating Systems** for MS Windows NT, Linux, or OS X. In **MS Windows 2000 or newer** mode the remote mouse is always synchronized with the local mouse.

### Mouse Speed

- **Auto mouse speed** Use this option if the mouse settings on the host use an additional acceleration setting. The CAT-32 IP tries to detect the acceleration and speed of the mouse during the mouse sync process.
- **Fixed mouse speed** Use a direct translation of mouse movements between the local and the remote pointer.

You may also set a fixed scaling which determines the amount the remote mouse pointer is moved when the local mouse pointer is moved by one pixel. This option only works when the mouse settings on the host are linear. This means that there is no mouse acceleration involved.

To set the options, click on the **Apply** button.

### Video



### Miscellaneous Video Settings

#### Noise filter

This option defines how the CAT-32 IP reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). In general the default settings should be suitable for most situations.

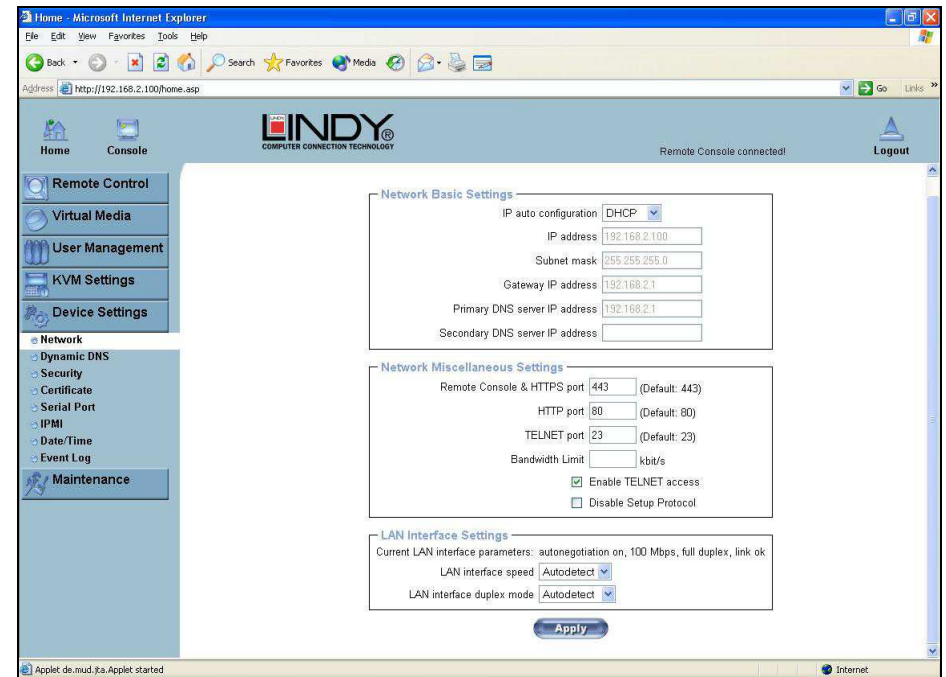
### Force Composite Sync (Required for Sun Computers)

To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the remote console will not be visible. To set the options, click **Apply**.

### 5.7.5. Device Settings

#### Network

The Network Settings panel allows network related parameters to be changed. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.



**Note:** The initial IP configuration is usually done directly at the host system using the special procedure in the beginning of Section 5.

Changing the network settings of the KVM over IP module might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the KVM over IP module.

**IP auto configuration**

With this option you can control if the CAT-32 IP should obtain its network settings from a DHCP or BOOTP server. For DHCP, select **dhcp**, and for BOOTP select **bootp**. If you choose **none** then IP auto configuration is disabled.

**IP address**

IP address in the usual dot notation.

**Subnet Mask**

The net mask of the local network.

**Gateway IP address**

In case the CAT-32 IP is accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

**Primary DNS Server IP Address**

IP address of the primary Domain Name Server in dot notation. This option may be left empty; however, the CAT-32 IP will not be able to perform name resolution.

**Secondary DNS Server IP Address**

IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

**Remote Console and HTTPS port**

Port number at which the CAT-32 IP's Remote Console server and HTTPS server are listening. If left empty the default value will be used.

**HTTP port**

Port number at which the CAT-32 IP's HTTP server is listening. If left empty the default value will be used.

**Telnet port**

Port number at which the CAT-32 IP's Telnet server is listening. If left empty the default value will be used.

**Bandwidth limitation**

The maximum network traffic generated through the CAT-32 IP's Ethernet device. Value in Kbit/s.

**Enable Telnet access**

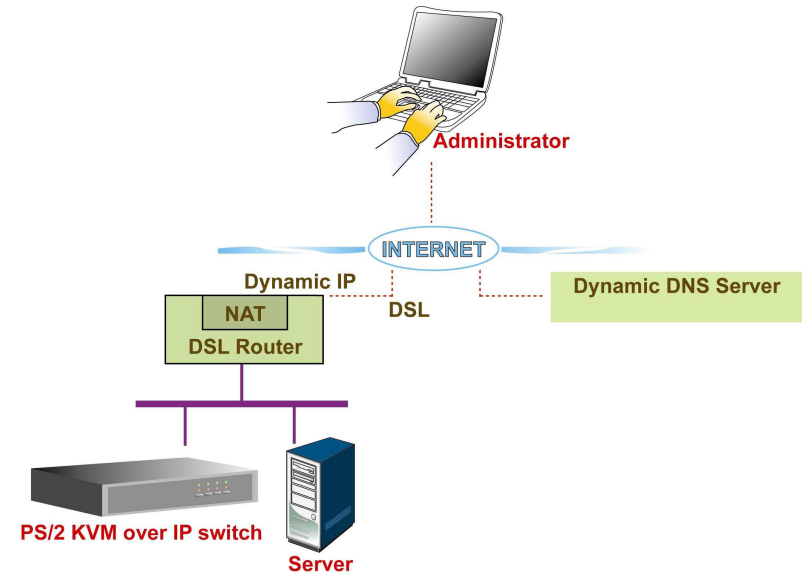
Set this option to allow access to ARA express using the Telnet Gateway (**see the Section called Telnet Console**)

**Disable Setup Protocol**

Enable this option to exclude the CAT-32 IP from the setup protocol.

**Dynamic DNS**

A freely available Dynamic DNS service (dyndns.org) can be used in the following scenario (see illustration below)

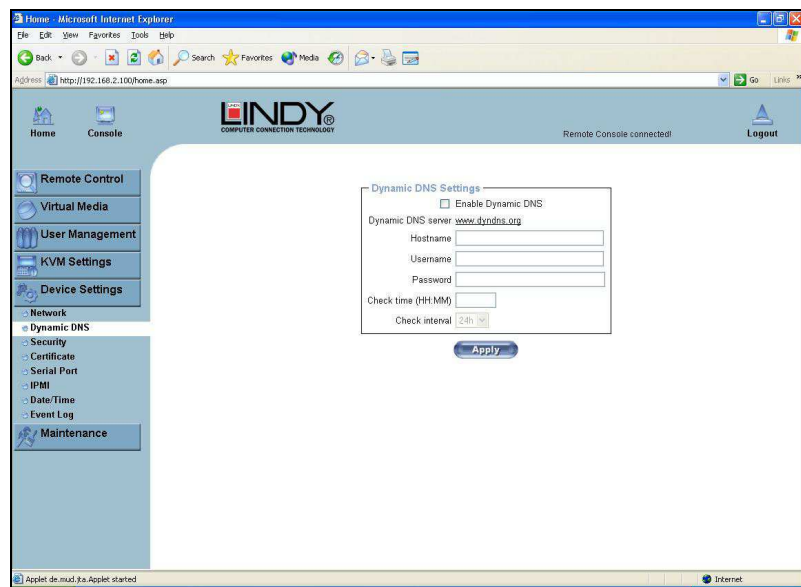


The CAT-32 IP is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the CAT-32 IP connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his device.

The administrator has to register a CAT-32 IP that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return. This account information, together with the hostname, is needed in order to determine the IP address of the registered CAT-32 IP.

You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the CAT-32 IP is properly configured.
- Open the Dynamic DNS Settings configuration dialog
- Enable Dynamic DNS and change the settings according to your needs (see the next page).



### Enable Dynamic DNS

Enables the Dynamic DNS service. This requires a configured DNS server IP address.

### Dynamic DNS server

This is the server name where the CAT-32 IP registers itself in regular intervals. At the time of writing, this is a fixed setting since only dyndns.org is currently supported.

### Hostname

This is the hostname of the CAT-32 IP that is provided by the Dynamic DNS Server. (Use the whole name including the domain, **e.g. testserver.dyndns.org** not just the actual hostname).

### Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the nickname.

### Password

The password used during manual registration with the Dynamic DNS Server.

### Check time

The CAT-32 IP registers itself in the Dynamic DNS server at this time.

### Check interval

This is the interval for reporting again to the Dynamic DNS server by the CAT-32 IP.

**Note:** The KVM over IP module has its own independent real time clock. Make sure the time setting is correct. (See the Section called Date and Time on page 59)

## Security



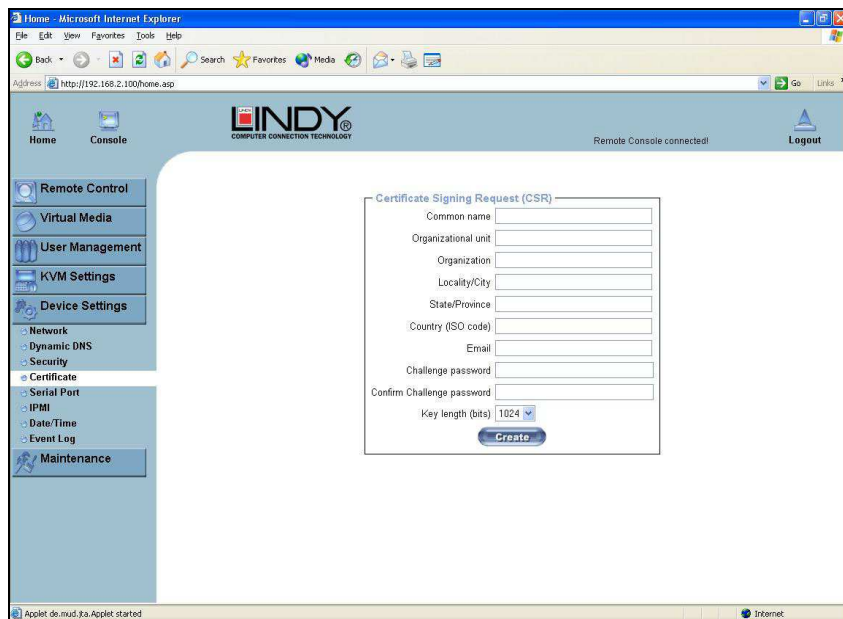
### Force HTTPS

If this option is enabled, access to the web front-end is only possible using an HTTPS connection. The CAT-32 IP will not listen on the HTTP port for incoming connections.

### KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator's machine and the keyboard and mouse data back to the host. If set to "Off" no encryption will be used. If set to "Try", the applet will attempt to establish an encrypted connection. If connection establishment fails for any reason an unencrypted connection will be used. If set to **Force** the applet tries to make an encrypted connection. An error will be reported if connection establishment fails.

## Certificate



The CAT-32 IP uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the CAT-32 IP has to expose its identity to a client using a cryptographic certificate.

This certificate and the underlying secret key is the same for all CAT-32 IP units and certainly will not match the network configuration that will be applied to the CAT-32 IP by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).

However, it is possible to generate and install a new certificate that is unique for a particular CAT-32 IP. In order to do this, the CAT-32 IP is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person you claim you are, and signs and issues a SSL certificate to you.

The following steps are necessary to create and install an SSL certificate for the CAT-32 IP:

1. Create an SSL Certificate Signing Request using the panel shown in the screen shot above. You need to fill out a number of fields that are explained on the next page. Once this is done, click on the **Create** button to initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the **Download CSR** button (see the illustration on the next page).
2. Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
3. Upload the certificate to the CAT-32 IP switch using the **Upload** button.

**Certificate Signing Request (CSR)**

The following CSR is pending:

countryName	= TW
stateOrProvinceName	= taipei
localityName	= taipei
organizationName	= test org
organizationalUnitName	= test
commonName	= test
emailAddress	= test@test.com

**Download** **Delete**

---

**Certificate Upload**

SSL Certificate File  **Browse...**

**Upload**

After completing these three steps, the CAT-32 IP has its own certificate that is used to identify it to its clients.

**Note:** If you destroy the CSR on the KVM over IP module there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described previously.

### Common name

This is the network name of the CAT-32 IP once it is installed in the user's network. It is identical to the name that is used to access the CAT-32 IP with a web browser (without the "http://" prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the CAT-32 IP is accessed using HTTPS.

### Organizational unit

This field is used for specifying to which department within an organization the CAT-32 IP belongs.

### Organization

The name of the organization to which the CAT-32 IP belongs.

### Locality/City

The city where the organization is located.

### State/Province

The state or province where the organization is located.

### Country (ISO code)

The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA.

### Challenge Password

Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters.

**Confirm Challenge Password**

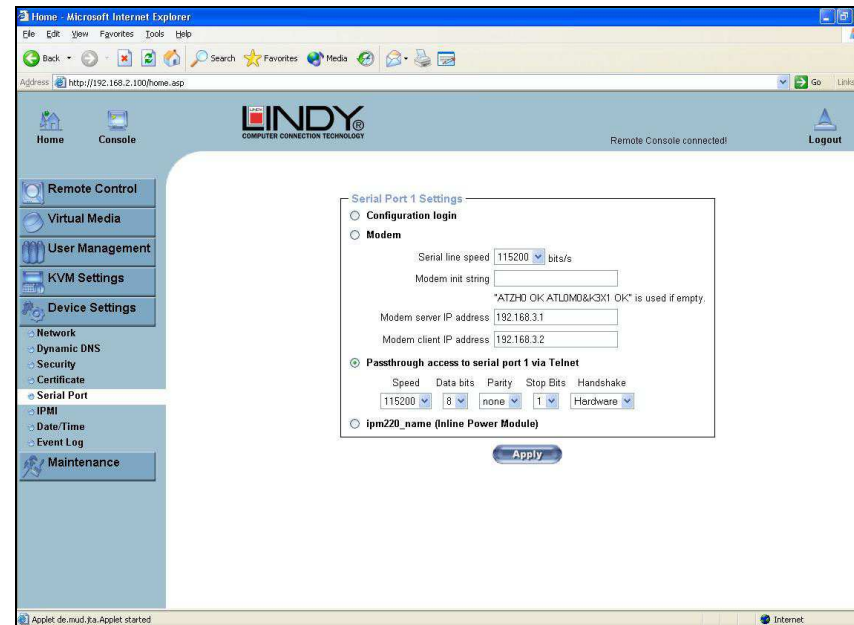
Confirmation of the Challenge Password

**Email**

The email address of a contact person that is responsible for the CAT-32 IP and its security.

**Key length**

This is the length of the generated key in bits. 1024 bits are sufficient for most cases. Longer keys may result in slower response time by the CAT-32 IP during connection establishment.

**Serial Port**

The CAT-32 IP Serial Settings allow you to specify what device is connected to the serial port and how to use it.

**Configuration or console login**

Do not use the serial port for any special function; use it only for the initial configuration

**Modem**

The CAT-32 IP offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the CAT-32 IP.

Connecting to the CAT-32 IP using a telephone line allows you to set up a dedicated point-to-point connection from your console computer to the CAT-32 IP. In other words, the CAT-32 IP acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the CAT-32 IP, make sure you configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection, which defaults to the right settings like PPP.

The Modem Settings panel allows you to configure remote access to the CAT-32 IP using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel.



### Serial line speed

The speed the CAT-32 IP is communicating with the modem. Most modems available today will support the default value of 115200 bps. In case you are using an old modem and discovering problems try to lower this speed.

### Modem Init String

The initialization string used by the CAT-32 IP to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by entering a new string. Refer to your modem's manual about the AT command syntax.

### Modem server IP address

This IP address will be assigned to the CAT-32 IP during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of the CAT-32 IP and your console computer. The default value will work in most cases.

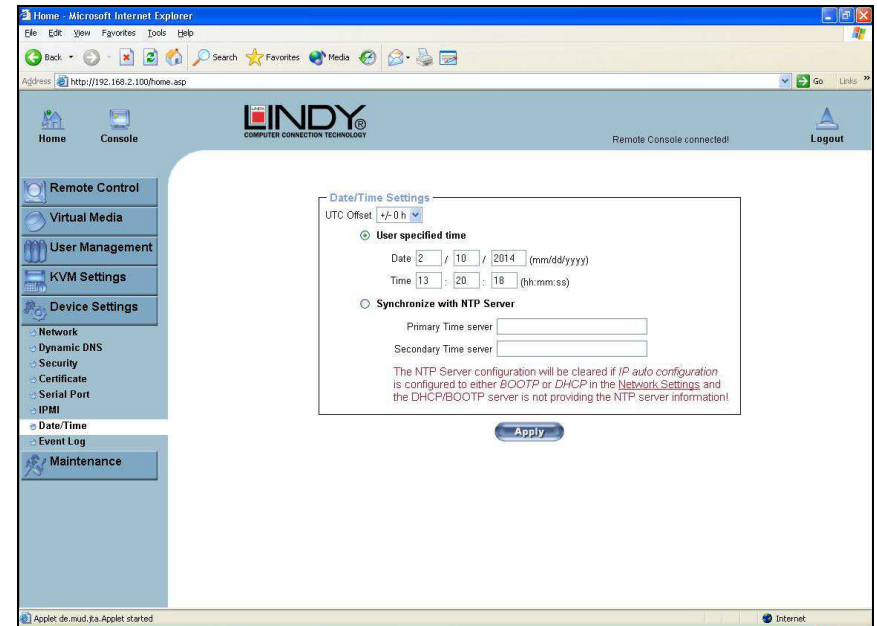
### Modem client IP address

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of the CAT-32 IP switch and your console computer. The default value will work in most cases.

### Pass-through access to serial port via Telnet

Using this option, it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port and use the Telnet Console, or a standard Telnet client to connect to the CAT-32 IP.

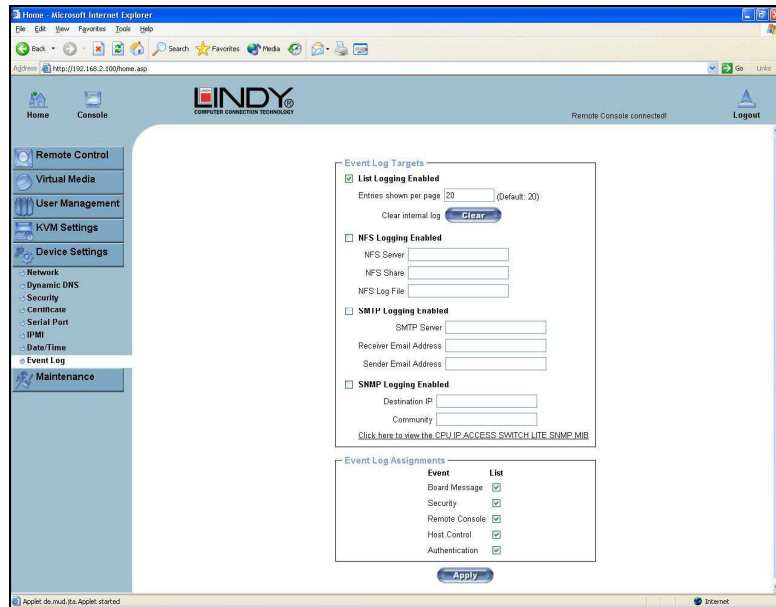
## Date And Time



Here you can set the internal real-time clock of the CAT-32 IP. You can adjust the clock manually or use an NTP timeserver. Without a timeserver your time setting will be lost if the CAT-32 IP is powered down for more than a few minutes. To avoid this, you can use an NTP timeserver which sets up the internal clock automatically to the current UTC time. Because the NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

**Note:** The KVM over IP module does not adjust to daylight saving time automatically. So you have to set up the UTC offset according to the local conventions of your country.

## Event Log



Important events like a login failure or a firmware update are logged to a selection of logging destinations. Each of those events belongs to an event group, which can be activated separately.

In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

### List logging enabled

The common way to log events is to use the internal log list of the CAT-32 IP. To show the log list, click on **Event Log** on the **Maintenance** page.

Since the CAT-32 IP's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1000 events. Every entry that exceeds this limit overrides the oldest one.

**Note:** If the reset button on the HTML front end is used to restart the KVM over IP module all logging information is saved permanently and is available after the module has been started. If the KVM over IP module loses power or a hard reset is performed, all logging data will be lost. To avoid this, use one of the log methods described below.

### NFS Logging enabled

Defines an NFS server to write all logging data to a file that is located there. To write logging data from multiple CAT-32 IP units to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press **Apply**, the NFS share will be mounted immediately. That means, the NFS share and the NFS server must be filled with valid sources or you will get an error.

### SMTP Logging enabled

With this option, the CAT-32 IP is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify an SMTP server that has to be reachable from the CAT-32 IP and that needs no authentication at all (<serverip>:<port>).

### SNMP Logging enabled

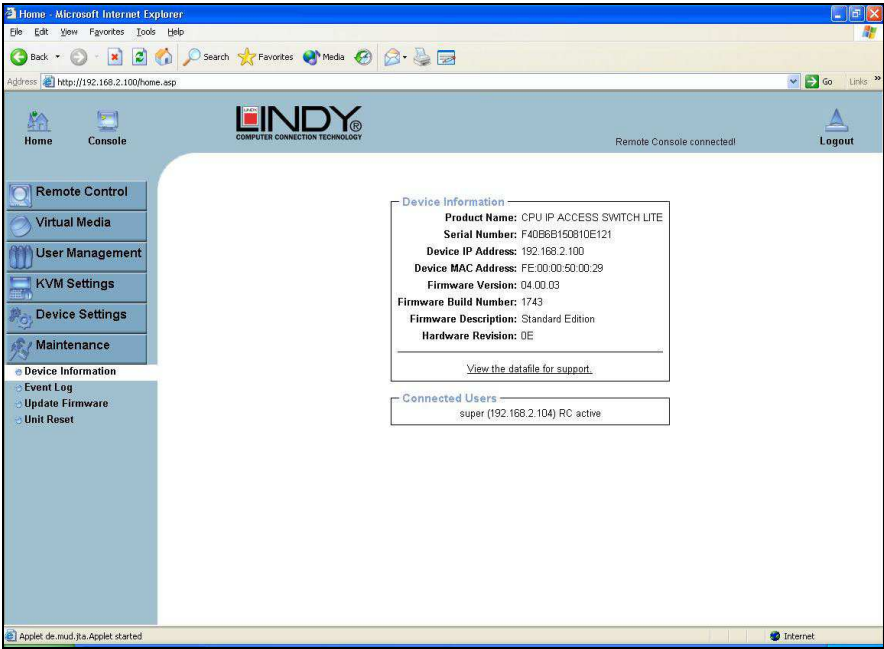
If this is activated, the CAT-32 IP sends an SNMP trap to a specified destination IP address every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have a trap class that consists of several fields with detailed information about the occurred event. To receive these SNMP traps, any SNMP trap listener may be used.

**Warning** In contrast to the internal log file on the CAT-32 IP, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously, so you may have to delete it or move it from time to time.

5.7.6. Maintenance

Device Information

This section contains a summary showing various information about the CAT-32 IP and its current firmware. It also allows you to reset the unit.



View the data file for support

Allows you to download the CAT-32 IP data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You can send this information if you contact LINDY technical support. It may help us solve any problems.

Connected Users

The example below displays the CAT-32 IP activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. **RC** means that the Remote Console is open. If the Remote Console is opened in exclusive mode the term (exclusive) is added. For more information about this option see the section called Remote Console Control Bar.

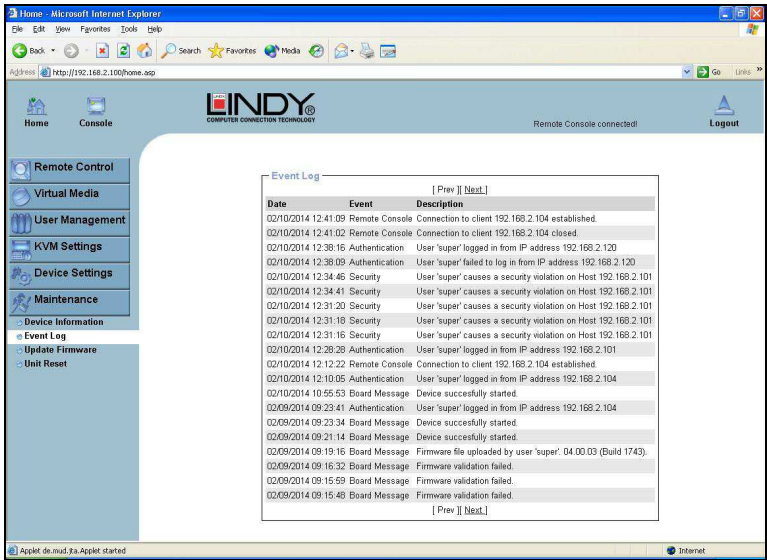
To display the user activity, the last column contains either the term **active** for an active user or **20 min idle** for a user who is inactive for a certain amount of time.

Connected Users

test (62.238.0.39)	active
test (80.145.25.183)	26 min idle
test (212.183.10.29)	20 min idle
test (62.153.241.228) RC (exclusive)	active

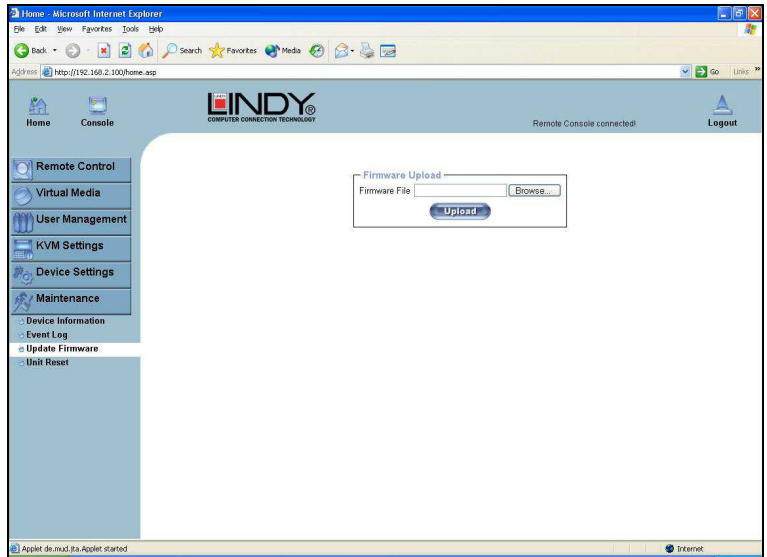
Event Log

Displays the log list including the events that are logged by the CAT-32 IP.



Update Firmware

The CAT-32 IP is a complete standalone computer. The software it runs is called the firmware. The firmware of the CAT-32 IP can be updated remotely in order to install new functionality or special features.





New firmware updates are provided as a binary file which can be sent to you by email. Please contact LINDY Technical Support team in your preferred country should you need to update your firmware. Please note that an error during a firmware update may cause damage to the unit, therefore a firmware update should only be performed if it is really necessary.

Updating the firmware is a four stage process:

1. The new firmware file is uploaded to the CAT-32 IP. In order to do this you need to select the file on your local system using the **Browse** button on the Upload Firmware panel. Once the firmware file has been uploaded it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted.
2. If everything went well you will see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the **Update** button will replace the old version with the new one.
3. After the firmware has been stored, the CAT-32 IP will automatically reset itself. Half a minute after the reset the CAT-32 IP will run with the new firmware version and should be accessible. However, you will be required to login once again.
4. Once you have logged in we recommend you delete the **Temporary Internet Files** from your browser to ensure that the appearance of the web interface is correct. To do this in Internet Explorer, select:

**Tools > Internet Options > General > Delete Files**

Tick the check box: **Delete all offline content**, and click **OK**

**Note:** The firmware update process and consistency check means that making a mistake when updating the firmware is very unlikely. However, we recommend only experienced users or administrators should perform the firmware update. This process is not reversible and may take some minutes. Make sure the Cat-32 IP's power supply will not be interrupted during the update process!

**Tip:** Should your keyboard fail to operate correctly, in the remote console, after a firmware update please use the **Reset Keyboard/Mouse** option in the **Maintenance** section.

## Unit Reset

This section allows you to reset specific parts of the device. This involves the keyboard and mouse, the video engine and the CAT-32 IP itself.



Resetting the unit itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console.

The whole process will take about half a minute. Resetting sub devices (e.g. the video engine) will take a few seconds only and does not result in connections closing. To reset individual CAT-32 IP functionality, click on the Reset button.

**Note:** Only the super user is allowed to reset the CAT-32 IP.

# Troubleshooting

## KVM Switch Troubleshooting

If none of the port LEDs or the display on the KVM Switch are illuminated then please check that the power adapter is connected and switched on at the mains.

**Before you check any further please make sure that all cables are fitted correctly!**

1. If the problem is also visible from the local console please first refer to section 3.4 Troubleshooting.
2. Please check if the currently selected computer is in sleep mode or powered down.
3. If the Monitor picture is not sharp or shows shadows: Please check the quality of the UTP cable between KVM switch and Computer Access Module. Try replacing the cable, or use a higher quality cable.
4. If you have forgotten a **Password** please contact LINDY.

## IP Access Troubleshooting

1. **The remote mouse doesn't work or is not synchronized**  
Make sure the mouse settings in CAT-32 IP match the mouse model. Use the **Intelligent Sync** option from the **Mouse Handling** sub menu of the Remote Console **Options** menu.
2. **The remote mouse does not work correctly**  
Try using the **Reset Keyboard/Mouse** option in the **Maintenance** section.
3. **The video quality is bad or the picture is grainy**  
Try to correct the brightness and contrast settings until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.
4. **Login on CAT-32 IP switch fails.**  
Was the correct combination of user and password given? The default user name is **super** and the password is **pass**. Furthermore, your browser must be configured to accept cookies.
5. **The Remote Console window can't connect to the CAT-32 IP.**  
Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connections. Install the latest version of Java Virtual Machine.
6. **No connection can be established to the CAT-32 IP.**  
Check whether the network connection is working in general (ping the IP address of CAT-32 IP). If not, check the network hardware. Is the CAT-32 IP powered on? Check whether the IP address of CAT-32 IP switch and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, including routers etc., is correctly configured.

7. **Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.**  
You have to define a so-called **Button Key**. This can be done in the Remote Console settings.

8. **In the browser the CAT-32 IP switch pages are inconsistent.**  
Clear **Temporary Internet Files** from your browser. To do this in Internet Explorer, select:

**Tools > Internet Options > General > Delete Files**

Tick the check box: **Delete all offline content**, and click **OK**

9. **Windows XP doesn't wake from standby mode**  
This could be a Windows XP problem. Try not to move the mouse while XP goes into standby mode.
10. **Every time I open a dialog box with some buttons, the mouse pointers are not synchronised anymore**  
Please check if you have an option like '**Automatically move mouse pointer to the default button of dialog Unites**' enabled in the mouse settings of the operating system. This option needs to be disabled.

# Key Codes

This table shows the key codes used to defines keystrokes or hotkeys for several functions. Please note that these key codes do not necessarily represent key characters that are used on international keyboards. They name a key on a standard 104 key PC keyboard with US English language mapping.

0 - 9
A - Z
, TILDE
- , MINUS
=, EQUALS
.
<, LESS
.
/, SLASH
BACK SPACE
TAB
[
]
ENTER
CAPS LOCK
\, BACK SLASH
LSHIFT, SHIFT
RCTRL
RSHIFT
LCTRL, CTRL
LALT, ALT
SPACE
ALTGR
ESCAPE, ESC
F1
F2
F3
F4
F5
F6
F7
F8
F9
F10
F11
F12
PRINTSCREEN
SCROLL LOCK
BREAK
INSERT
HOME
PAGE UP
DELETE
END
PAGE DOWN
UP
LEFT
DOWN
RIGHT
NUM LOCK
NUMPAD0
NUMPAD1
NUMPAD2
NUMPAD3
NUMPAD4
NUMPAD5
NUMPAD6
NUMPAD7
NUMPAD8
NUMPAD9
NUMPADPLUS,NUMPAD PLUS
NUMPAD/
NUMPADMUL,NUMPAD MUL
NUMPADMINUS,NUMPAD MINUS
NUMPADENTER
WINDOWS
MENU

The layout for this keyboard is also shown. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are in an identical position, no matter what language mapping you are using. Some of the keys have aliases also; they can be named by 2 key codes (separated by a comma in the previous table).

Esc	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	Prnt	Scr1	Brk					
~	1	2	3	4	5	6	7	8	9	0	-	=	Bsp	Ins	Pos1	Pgup	Num	/	*	-
tab	q	w	e	r	t	y	u	i	o	p	[	]	CR	Del	End	Pgdn	7	8	9	+
Caps	a	s	d	f	g	h	j	k	l	;	'	\		4	5	6				
LShift	z	x	c	v	b	n	m	,	.	?	Rshift			Up			1	2	3	CR
Lctrl	Win	Alt	Space					AltGR	Menu	RCtrl	Left	Down	Right	0	,					

# Video Modes

The table below lists the video modes that the CAT-32 IP remote console supports. Please do not use any other custom video settings; the CAT-32 IP may not be able to detect them.

Resolution (x, y)	Refresh Rates (Hz)
640 x 350	70, 85
640 x 400	56, 70, 85
640 x 480	60, 67, 72, 75, 85, 90, 100, 120
720 x 400	70, 85
800 x 600	56, 60, 70, 72, 75, 85, 90, 100
832 x 624	75
1024 x 768	60, 70, 72, 75, 85, 90, 100
1152 x 864	75
1152 x 870	75
1152 x 900	66
1280 x 960	60
1280 x 1024	60, 75

Higher resolutions than 1280 x 1024, i.e. 1600x1200 may be displayed in virtual desktop mode with a moving visible area of 1280 x 1024.

## WEEE (Waste of Electrical and Electronic Equipment), Recycling of Electronic Products



### United Kingdom

In 2006 the European Union introduced regulations (WEEE) for the collection and recycling of all waste electrical and electronic equipment. It is no longer allowed to simply throw away electrical and electronic equipment. Instead, these products must enter the recycling process.

Each individual EU member state has implemented the WEEE regulations into national law in slightly different ways. Please follow your national law when you want to dispose of any electrical or electronic products.

More details can be obtained from your national WEEE recycling agency.

### Germany / Deutschland

Die Europäische Union hat mit der WEEE Richtlinie umfassende Regelungen für die Verschrottung und das Recycling von Elektro- und Elektronikprodukten geschaffen. Diese wurden von der Bundesregierung im Elektro- und Elektronikgerätegesetz – ElektroG in deutsches Recht umgesetzt.

Dieses Gesetz verbietet vom 24.März 2006 an das Entsorgen von entsprechenden, auch alten, Elektro- und Elektronikgeräten über die Hausmülltonne! B2B Geräte wie diese KVM Switches nimmt LINDY kostenlos zurück und führt sie einem geordneten Recycling zu. Bitte nehmen Sie hierzu Kontakt mit LINDY auf, die Adressen finden Sie auf der LINDY Website [www.lindy.com](http://www.lindy.com)

### France

En 2006, l'union Européenne a introduit la nouvelle réglementation (DEEE) pour le recyclage de tout équipement électrique et électronique.

Chaque Etat membre de l' Union Européenne a mis en application la nouvelle réglementation WEEE de manières légèrement différentes. Veuillez suivre le décret d'application correspondant à l'élimination des déchets électriques ou électroniques de votre pays.

### Italy

Nel 2006 l'unione europea ha introdotto regolamentazioni (WEEE) per la raccolta e il riciclo di apparecchi elettrici ed elettronici. Non è più consentito semplicemente gettare queste apparecchiature, devono essere riciclate.

Ogni stato membro dell' EU ha tramutato le direttive WEEE in leggi statali in varie misure. Fare riferimento alle leggi del proprio Stato quando si dispone di un apparecchio elettrico o elettronico.

Per ulteriori dettagli fare riferimento alla direttiva WEEE sul riciclaggio del proprio Stato.

## CE Statement

This device complies with the European Regulations for Electromagnetic Compatibility (EMC) of the European Union and it is equipped with the CE mark. This unit has to be used with high quality shielded connection cables. Only if these high quality shielded cables are used can it be sure that the EMC compatibility is not adversely influenced.

## FCC Statement

Shielded cables must be used with this equipment to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

### FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.